Report

of the Executive Committee

Privacidad y tecnología en equilibrio

34° Conferencia Internacional de Autoridades de PROTECCIÓN DE DATOS Y PRIVACIDAD

During the 33rd International Conference, held in 2011 in Mexico City, it was decided to install an Executive Committee. According to the Rules of Procedure, the International Conference consists of the Closed Session, the Executive Committee and the Working Groups. The Hosting Authority is free to organize in addition to the Closed Session an open meeting as well. Such an open meeting is however not a formal part of the International Conference.

It is the task of the Executive Committee to manage and represent the International Conference. Therefore the Committee shall ensure that the decisions taken during the Closed Session are implemented and that resolutions are implemented. Furthermore, the Committee shall assist the Hosting Authority in organising the Annual Meeting (i.e. the Closed Session).

The report in front of you contains the results of the first year's work of the Executive Committee. Six meetings have been held: three face-to-face (in Mexico City, Montréal and Punta del Este) and three telephone conferences. During these meetings, the Committee primarily discussed the preparations for the 2012 Closed Session, including the identification of a suitable topic to be discussed and relevant speakers. Furthermore, attention was paid to the accreditation of new members and the representation of the Conference to international organisations and other fora.

Membership & Division of tasks

The current Executive Committee comprises five members, as required by the Rules of Procedure. The membership and their current division of rotating tasks is as follows:

Permanent Members	
Dutch Data Protection Authority (NL)	Chair
Federal Trade Commission (USA)	Accreditations
Office of the Australian Information Commissioner (AUS)	Representation
Rotating Members	
Federal Institute for Access to Information and Data Protection (MX)	Host 2011
Regulatory and Control Unit for Data Protection (UY)	Host 2012

Preparations of the Closed Session

During the 2011 Closed Session, the members agreed to go back to basics and to make the Closed Session the heart of the International Conference again. The meeting should provide an opportunity for data protection and privacy enforcement authorities from around the world to discuss among each other current developments in their respective

fields of work, ongoing concerns and possible solutions. Furthermore, they should be able to make decisions on joint initiatives to improve and enhance enforcement actions.

Bearing this in mind, the Executive Committee decided in its first meeting to extend the Closed Session to one day and a half, in order to allow for a full day of discussions focussing on a specific topic. The topic should regard a new technique, application, etc. that almost all DPAs will have to deal with at some point in the near future. Upon a suggestion by the Chair, the Executive Committee decided in its second meeting that the topic to be discussed in 2012 would be profiling. You will read more on the background of this choice in the next section.

The Executive Committee also decided that in order to have a substantial debate, several speakers would be invited to put perspective on the issue based on real life experience. Together, the speakers would ideally be able to present an overview of developments on several continents in both the private (commercial) sector and the public (government) sector. Their presentations should be oriented at, but not limited to, data protection and privacy.

Especially thanks to the suggestions of the FTC, a long list of possible speakers was drawn up, four of which have agreed their willingness and ability to join us in Punta del Este.

Selection of this year's topic: profiling

The central topic identified by the Executive Committee to be discussed this year is profiling. Profiling is used, amongst others, to help organisations and companies target persons who may be of interest to them, whether these are potential customers, criminals, persons who may need healthcare, potential employees or others.

Profiling may be used to identify and contact persons both in a positive and in a negative sense. Companies may offer individuals special promotions, based on a profile of their purchases. Insurance companies on the other hand may require extra fees if the profile indicates a high risk lifestyle.

Given the discussions in Mexico City about big data, the Executive Committee considers profiling to be a perfectly fit topic for discussions between data protection and privacy commissioners. After all, in order to effectively draw up profiles, big data is needed.

For example, cyberspace is an environment where big data makes it possible to remember what a person has done and forecast what his/her behaviour will be. Through computer programs consisting of computational algorithms, a self-learning and self-correcting computer model can be created. By feeding back new data into the computer model, a more and more accurate forecast may arise.

As demonstrated at last year's Future of Privacy Forum in Washington, Google's translation service is a state of the art example of the potential of big data when enriched with feedback data. Today the self-learning algorithms powering the translation service support 63 languages.

Releasing this approach of enriching the potential of big data by adding feedback data, thereby improving the ability for example to forecast personal preferences, adjust pricing, predict medical problems or risky behaviour, shows what technology can bring to society in the future.

Societal risks
Profiling has implications for fundamental freedoms in general. The rights to fair and equal treatment and to non-discrimination might be jeopardised by the technique of profiling.

For example, we are now classified based on our profiles (young mothers, sport fans, smokers and shopaholics, etc.). Such pigeonholing may make any notion of freedom of choice illusory. A society divided by profiles challenges the freedom to progress in life and make new choices, without being forever held back by old ones.

By protecting personal data, we as regulators might be able to diminish the risk of large scale interference with fundamental freedoms, which are the basis of our modern democratic societies. When power combined with the possibility to collect and process personal data leads to an unreasonable limitation of the free development of people, watchdogs must bark and if need be bite.

Potential Benefits
Profiling can be very useful to find the proverbial needle in the ever bigger haystacks of data. If used correctly and taking into account data protection safeguards, it may even be a way to limit data processing operations.

For example, profiling by police and law enforcement may lead to a more secure society. And profiling by companies may make our day-to-day life easier, because it offers us advertisements of services and goods we would potentially be interested in, instead of adverts that are absolutely not of any interest to the data subject. Lastly, the use of profiles could save the private sector money and consequently may make some goods and services in the end cheaper for customers (or the profits for companies higher).

Data Protection and Data Accuracy Risks
Big data leads to many risks with regard to security, because the more data is stored, the bigger the risks and negative consequences by a loss or destruction of the data. In addition, big databases that are used for profiling run the risk of not containing correct and up to date information, which greatly influences the correctness and reliability of the profile(s) as a result. This may lead to false positives, even if the criteria used to draw up the profile are carefully chosen and applied.

Applicability
Because of the broad usability of this technique, profiling has implications for both the private sector and public sector and is therefore suitable for discussions regarding both sectors. Profiling leads to large scale data processing operations and could be of great influence on the private lives of individuals. This is especially true if automated decisions are taken which are only based on profiling information, for example decisions to require additional security checks or to exclude people from insurance.

In order to streamline the four contributions, the Executive Committee has asked the speakers to concentrate on two central questions.

1. What data are collected by whom in order to make what kind of profiles?
2. How effective are these profiles?

Permanent Conference Website

Next to its work in preparing the 2012 Closed Session, the Executive Committee also looked at the implementation of past decisions of the Conference. One of the open issues to be discussed, was the decision from the 2009 Closed Session (Madrid) to set up a permanent website for the Conference, to be hosted by the OECD.

The Executive Committee has consulted both the OECD and the Office of the Privacy Commissioner of Canada – in the past responsible for a working group on the introduction of a permanent website – on the state of play regarding the website. The situation appeared to be rather complex. Notwithstanding the past decision of the Conference that the OECD would host the website, the OECD in fact indicated to have no possibility to do so, since the website would not primarily be enforcement related. This was a precondition for an OECD-hosted permanent website, like the one for the Global Privacy Enforcement Network (GPEN). Furthermore, since the Conference has no legal personality it would be difficult to agree a Memorandum of Understanding with a hosting party.

Another challenge the Executive Committee identified for setting up a permanent website is the cost. Given the wish list of the Conference to set up the website with both publicly accessible information and a restricted, private space intended for secure information sharing between data protection and privacy enforcement authorities, a complex technical infrastructure would be required. This made alternative solutions – for example a website based on easily accessible blog software like Wordpress or Tumblr – impossible or at least improbable. A permanent website would thus require a professional hosting contract, including the subsequent costs. The Conference however has no financial means of itself to make any commitments for this purpose.

The Executive Committee has therefore come to the conclusion over the past year that it would be too difficult to make arrangements for a permanent website. It recommends that for the meantime, the Conference should continue to work the way we have done over the past years: the host country provides for a website for the next conference, and ensures that all relevant documentation from past years conferences – including resolutions, the rules of procedures and the forms to apply for membership or observer status – is available. So far, this practice has proved to be very effective and successful.

Accreditation

Within the Executive Committee, the Federal Trade Commission has assumed the responsibility to lead the accreditation process of new members and observers. Following modifications made to the Rules of Procedure during the 2011 Closed Session,

the application forms for both membership and observer status were updated in the first quarter of the year.

In the course of the year twelve applications for membership and/or observer status were received from authorities from all continents. Upon review of the applications received and consideration of the legislative instruments and other documents provided as background information, the Executive Committee agreed to recommend that the Colombia Superintendence of Industry and Commerce of Colombia, the Costa Rica Agencia de Protección de Dados de los Habitantes, The Korea Personal Information Protection Commission (PIPC), the Norway Datatilsynet, the Peru National Authority for Data Protection, the Saxon Commissioner for Data Protection, the Serbia Commissioner for Information of Public Importance and Personal Data Protection, and the Tunisia Instance Nationale de Protection des Données à Caractère be granted Member status to the Conference. The Executive Committee is satisfied that each of these authorities meets the requisite conditions for accreditation; notably that they:

- are public entities, created by an appropriate legal instrument based upon legal traditions of the country or international organization which they belong to;
- have the supervision of the implementation of the legislation on the protection of personal data or privacy as one of their principal regulatory mandates;
- operate under a legislation that is compatible with the principal international instruments dealing with data protection or privacy;
- have an appropriate range of legal powers to perform their functions; and
- have appropriate autonomy and independence.

The Executive Committee furthermore agreed to recommend that the Korea National Information Society Agency, The French-Speaking Association of Personal Data Protection Authorities, and The Organization of American States be granted Observer status to the conference, insofar as they are public entities involved in dealing with the protection of personal data.

Finally, and given that the Ecuador DINADARP has submitted its documentation significantly after the expiry of the deadline provided for by the Accreditation rules, the Executive Committee was not able to properly assess its membership application. However, it was agreed to recommend that DINADARP be approved as an observer, for they meet the criteria.

Detailed information on this year's applicants for membership and observer status is available in the Accreditation Resolution.

Representation to International Organisations

The Office of the Australian Information Commissioner has taken up the task to coordinate the representation of the International Conference to several international organisations. The Conference has been represented over the last couple of years at APEC, the Consultative Committee on Convention 108 of the Council of Europe, ISO and the OECD.

The 30th Conference established the Steering Group on Representation before International Organisations. The Steering Group has the task of arranging observer

representation before relevant international meetings in order to influence data protection policy formulation and to keep the Conference better informed.
The Steering Group's first report outlined in detail the establishment and operation of the Steering Group. It set out key processes and resources such as the 'expectations of delegates' document approved by the Steering Group.

The 33rd International Conference established a new governance structure for the Conference, including an Executive Committee. The Conference transferred to the Executive Committee responsibility for appointing 'delegates representing the Conference to those forums and/or international organisations in which the Conference has observer status'.

During the reporting period (October 2011 to October 2012), the Executive Committee maintained the former Steering Group's focus upon four principal international organisations:

- APEC — on 10 May 2012, the APEC Secretariat informed Executive Committee member Timothy Pilgrim (Office of the Australian Information Commissioner) that the Conference's guest status in APEC Electronic Commerce Steering Group (APEC ECSG) had been approved. The guest status is valid until 31 December 2014.
- Council of Europe — the Conference has observer status before the Consultative Committee on Convention No. 108 (T-PD)
- International Organisation for Standardisation — there has been an exchange of liaison officers between ISO and the Conference
- Organisation for Economic Cooperation and Development – the Conference has observer status before the Working Group on Information Security and Privacy (WPISP).

Meetings attended during the reporting period included:
- T-PD meeting, 19–22 June 2012, Strasbourg Switzerland
- APEC ECSG Data Privacy Subgroup meeting, 22–27 May 2012, Kazan Russia
- T-PD meeting, 6–8 February 2012, Strasbourg Switzerland
- APEC ECSG Data Privacy Subgroup meeting, 30 January–1 February 2012, Moscow Russia
- WPISP meeting, 1–2 December 2011, Paris France
- ISO Technical Management Board Privacy Steering Committee, 1–2 December 2011, Geneva Switzerland
- T-PD meeting, 29 November–2 December 2011, Strasbourg Switzerland

Conference delegates generally provide reports on meetings attended. These reports are then circulated to Executive Committee members and Steering Committee. In the next reporting period the Executive Committee will consider the wider distribution of these reports to DPAs. In the absence of a permanent Conference website, the Executive Committee will consider a range of options, including circulation of reports via email to Conference delegates and uploading meeting reports to existing websites, such as the Global Privacy Enforcement Network (GPEN) website (www.privacyenforcement.net/).
The Executive Committee considered, but did not pursue, observer representation at the following forums during the reporting period:

- Internet Governance Forum (IGF)
- London Action Plan
- International Law Commission
- Internet Corporation for Assigned Names and Number (ICANN)
- International Telecommunication Union (ITU)
- United Nations Educational, Scientific and Cultural Organization (UNESCO).

The Steering Group holds an existing mandate from the Conference to seek observer representation at these forums.

As advised in the report last year, the main difficulty in pursuing further applications for observer status is the Conference's limited capacity to routinely send delegates to the relevant meetings. Existing obligations already stretch the capacities of the members of the Steering Group.

For the time being, the Executive Committee does not propose to seek further observer status unless a suitable person, from among the staff of member authorities, has first been identified as available to perform the duties of a delegate. If any data protection authority (DPA) has an interest in providing a delegate to any of the international bodies mentioned, they should contact Executive Committee member Timothy Pilgrim (Office of the Australian Information Commissioner) so that the processes for seeking observer status can be initiated.

The Executive Committee acknowledges the hard work of the Steering Group and existing Conference delegates. During the year, valuable work was undertaken by Steven Johnston (Office of the Privacy Commissioner of Canada), ISO Liaison Officer, and Anton Battesti, (Commission nationale de l'informatique et des libertés (CNIL)), delegate to T–PD and WPISP.

In addition, the Steering Group was able to arrange one-off guest status for a conference delegate before a meeting of the APEC ECSG. Florence Raynal (CNIL) represented the Conference at the meeting in Moscow in February 2012 and her contribution is also acknowledged.

The Executive Committee thanks Markus Heyder (Federal Trade Commission) who, at short notice, attended the APEC ECSG Data Privacy Subgroup meeting in Moscow in May 2012.

The Executive Committee also acknowledges the efforts of Dr Wojciech Wiewiórowski (Inspector General for Personal Data Protection) who acted as liaison between the Conference and the Commonwealth of Independent States Countries.

On behalf of the Executive Committee,
Jacob Kohnstamm
Chairman

The Hague, The Netherlands – September 2012