"Communicating Data Protection and Making It More Effective"

Origin of this initiative

This statement stems from the speech by Alex Türk, President of the French Data Protection Authority, on the occasion of a conference organised in Warsaw in May 2006 by the Inspector General for Data Protection in Poland, on the theme "Public Security and Privacy". Alex Türk then shared his deep concerns as to the challenges which DPAs are currently facing. He insisted on the absolute necessity that DPAs urgently adapt their action to address these challenges, for fear that the philosophy underlying data protection rules would rapidly be deprived of substance.

In the aftermath of this conference, the EDPS invited the CNIL to set up a joint initiative presenting the need for such urgent action to be presented at the London conference. The UK Information Commissioner immediately fully supported this initiative. This statement was drafted in close cooperation between these three DPAs.

By joining this initiative, the participating DPAs undertake to coordinate their actions with the following objectives:

- Develop communication activities on the basis of common ideas, some of which are expressed in the appended text;
- Adapt their practices and methods by thoroughly assessing their efficiency and effectiveness, and by reinforcing their capacities of technical expertise, anticipation of trends, and intervention in the technological field;
- Contribute to the institutional recognition of DPAs at the international level and promote involvement of other appropriate stakeholders at national and international levels.

Currently, the following DPAs have in principle expressed their support to this initiative :

- Commission nationale de l'informatique et des libertés (France)
- European Data Protection Supervisor (European Union);
- Information Commissioner (United Kingdom);
- Privacy Commissioner of Canada (Canada);
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Germany);
- Agencia Española de Protección de Datos (Spain);
- Garante per la Protezione dei Dati Personali (Italy) ;
- College Bescherming Persoonsgegevens (the Netherlands);
- Privacy Commissioner (New Zealand);
- Préposé fédéral à la protection des données et à la transparence / Eidgenössische Datenschutz und Öffentlichkeitsbeauftragte (Switzerland).

This joint initiative will be presented during the closed session of the International Conference of Data Protection and Privacy Commissioners in London on November 2-3. It is not drafted as a resolution. It will be presented as a joint initiative of CNIL, EDPS and UK Information Commissioner which the DPAs mentioned above support, thereby undertaking to adapt their action to take it into account. The other DPAs represented at the conference will be invited to express their support and may be even join this initiative if they so wish. They will however not be asked to formally adopt this document.

After recalling why data protection is indispensable to our societies (I), this text analyses in detail the risks which today weigh on individual liberties and data protection around the world, and which represent as many challenges for supervisory authorities (II). It derives from this statement various proposals for coordinated actions and initiatives (III), as well as for the development of a new common communication strategy (IV).

I – DATA PROTECTION IS INDISPENSABLE TO SOCIETY

1. The protection of citizens' personal data is vital for any society, on the same level as freedom of the press or freedom of movement. As our societies are increasingly dependent on the use of information technologies, and personal data are collected or generated at a growing scale, it has become more essential than ever, that individual liberties and other legitimate interests of citizens are adequately respected in relevant information practices.

2. Data protection is not, and must not be seen as, an abstract, theoretical, let alone a "theological" subject. *Data* protection rules are about the protection of *individuals*. They aim to uphold the right not to be on file or monitored in an abusive or uncontrolled manner. They aim to defend human dignity and to enable individuals to exercise their rights and protect their legitimate interests.

3. Data protection can only be made a reality, if data protection rules are complied with in practice. Data protection authorities have a key role in ensuring compliance, but they can only be successful if they are effective in communicating the data protection message and involving other appropriate stakeholders, and if necessary in using their powers of investigation and enforcement.

II – TWO WAVES; THREE CHALLENGES

4. Individual liberties, and data protection authorities themselves, are exposed to unprecedented risks. Two waves threaten to overwhelm them, but they also face a third challenge.

A –The first challenge flows from many different factors associated with the pace of technological change.

5. **Acceleration**: Internet, RFID, nanotechnologies etc. DPAs are not hostile to innovation or technological progress. But the period of time running from the discovery of a phenomenon to its technical implementation, from an innovation to another, from the development of a prototype to its industrial implementation is getting shorter and shorter. It is increasingly difficult for attempts at legal adaptation or construction to coincide with technological evolution. The technological pace keeps accelerating, while the legal pace remains particularly slow, as it is phased on the rhythm imposed by democratic procedures.

6. **Globalisation:** the relocation of data processing is in full boom. It is unquestionably very difficult to control international data transfers. This trend towards globalisation conflicts with one of the main characteristics of the rule of law, which is the geographically limited scope of its application.

7. **Ambivalence:** technological innovation brings about both progress and dangers. Individuals may be very tempted by the benefits and comfort provided by technology, but they may be

insufficiently aware of the risks until they or others suffer harm or it is too late. Many do not care about their traceability and the potential surveillance of all their movements, behaviours, or relationships. This ambivalence towards technology is difficult to reconcile with the rule of law which, by definition, seeks to provide "black and white" answers.

8. **Unpredictability:** technological uses often develop in a manner that was originally unpredictable, even by the designers of the technology. These unpredictable uses may thereby be difficult to regulate, especially when they completely diverge from the uses for which the technology was initially designed, and for which the law originally seemed easily applicable.

9. **Invisibility (virtual invisibility / physical invisibility)**: information processing is growing more and more invisible and intangible, but less and less controllable. Technology tends to invisibility, firstly because much data processing is carried out without individuals being aware of its existence (eg traceability in public transportation, of Internet surf, of electronic and phone communications, etc.) Here one may talk of virtual invisibility, because the processes are invisible. But technology also grows invisible because of its extreme miniaturization: one may then talk of real invisibility. In a few years, the development of nanotechnologies will make it impossible to see with the naked eye that technology is even present in an object. How will it be possible to monitor the development of processing operations carried out by invisible technologies?

10. **Irreversibility**: technological progress is irreversible: we shall never live any more in a world without computers, Internet, mobile phones, biometric identification, geolocalisation, CCTV. As these technologies converge and become ever-more interwoven, their combination could present real risks for our societies.

B – The second challenge is of a legal nature, especially related to the development of new anti-terrorism laws

11. The development of anti-terrorism laws sets a challenge to data protection authorities who, in this context, must avoid traps, denounce illusions and fight myths.

12. **The need for balance**: As neither lawmakers, nor courts, nor activists, independent data protection authorities nevertheless have a very specific role to play. It is rarely possible for them to resolve issues with a "black and white" approach. Thus all data protection authorities acknowledge the legitimacy of anti-terrorism policies which have been developed over the past years. Yet, in accordance with the missions which they were granted by law, and on behalf of society as a whole, it is their duty to constantly seek the right balance between the imperatives of public security on the one hand, and the imperatives of privacy and data protection, on the other hand. They must take up this role with full independence and resist unacceptable accusations of irresponsibility which are sometimes uttered against them.

13. **The danger of getting caught in a spiral system:** this risk – a type of "function creep" - is as follows. A database may be legally created at a given moment, under specific circumstances. The supervisory authority is associated to its development. Later, its scope expands - for example first extending the categories of persons concerned, then the reasons for being registered, and then later again the categories of persons allowed to have access to the database. In these later phases the authority faces the argument that it cannot oppose a simple extension, since it accepted the principle for the creation of the initial database, and so on if necessary. Yet, between the first and last phase of the development of that system, its originally acceptable perimeter will have shifted so much that it will have grown into the unacceptable.

14. **The illusion of the exemplary nature of foreign precedents:** national governments often use the argument that such and such a country has already put a system into place to attack their national data protection authorities for their reluctance to accept the same system without discussion. This causes serious problems of harmonisation and makes it necessary for DPAs to think together on the basis of common denominators.

15. **The mirage of the database as a miracle cure**: DPAs must constantly remind the public and governments that creating databases with ever-more personal information does not solve all problems. The sacred aura of the supposedly infallible computer file must often be portrayed as a delusion. In addition, as more and more personal information is processed, the risks increase of false matches, out of date information and other mistakes. These can cause real harm to the life chances, the health, the prosperity, and even the liberty, of individuals.

16. **The myth of the infallible file (the "majority / minority" issue)**: It is too often supposed – without foundation - that all individuals must be registered in a database for a valid reason. As a result, persons unnecessarily or improperly registered in such databases ("the minority") sometimes find themselves in impossible situations, since everyone believes that it is virtually impossible to be mentioned in such an efficient system without justification. It is therefore essential, from an ethical point of view, to keep affirming that technology is fallible and to forbid automatic decision making, especially in domains such as security and justice.

C – The third challenge is reputational

17. In some countries at least, data protection and DPAs do not enjoy the positive reputation they deserve. The rules can be seen as complex and difficult to apply in practice in consistent, predictable and realistic ways. Some criticise the regulation of data protection as excessively abstract, and not sufficiently focused on the actual or potential harms that can arise – to individuals and society at large - if the rules are not observed. Others criticise the way in which these rules are implemented and enforced, resulting in a lack of positive or negative incentives to comply or to invest in adequate compliance. Negative perceptions such as these can be held by politicians, administrators, businesses, the media and sometimes by private individuals. It is necessary to attack such perceptions, demonstrating the practical importance of data protection, making reality of the language of fundamental rights and freedoms, and to reconsider current practices, where appropriate.

III – LINES OF ACTION AND INITIATIVES FOR DPAs

18. Because of their seriousness, DPAs must urgently take action to awake their citizens to better awareness and understanding of the risks threatening individual liberties in their respective countries. They must also evaluate their working methods and improve their efficiency and effectiveness.

A – DPAs must together bring forward changes and coordinated strategies so as to act in new, more effective and more relevant ways

19. **Strengthen capacities of expertise, advanced studies and intervention in the technological field:** data protection currently suffers by its excessively « legal » image; yet the credibility of our institutions is, and will be more and more dependent on our capacity to understand, analyze and anticipate technological development.

20. To analyse these new trends, DPAs must elaborate strategies to share work among them depending on the issues of the case at hand, on their respective experiences and responsibilities and of their practical means of action.

21. They must reflect on the relationships which they wish to achieve with researchers and industry in the field of new technology. They must stress the benefits of good data protection to businesses and public bodies themselves.

22. **Assess our effectiveness and change our practices**: it is absolutely necessary to carry out a thorough and honest assessment of the effectiveness of each authority. Is each authority achieving a real impact, and making a real difference, in practice? Do words translate into actions? Such assessments will enable us to learn lessons as to how to improve our results.

23. The assessment of each authority's effectiveness will certainly lead some of them to claim from the lawmaker that they are granted sufficient powers and resources. It may also raise questions about some practices of some authorities. We must all prioritise, especially by reference to the seriousness and likelihood of harm. We must primarily concentrate on the main risks which individuals are now facing and be careful not to be excessively rigid or purist on issues which do not deserve it. We must be ready for more pragmatism and more flexibility.

B – DPAs must reflect together on how to obtain better institutional recognition of their action at the international level and to involve other stakeholders

24. **A necessary re-structuring of the International Conference:** Global challenges need global solutions. The International Conference of Data Protection and Privacy Commissioners must be the spearhead of our action at the international level. We must ensure its viability, improve its functioning, make it more visible and more efficient, and elaborate an action plan, a communication programme. This may imply thinking about the creation of a permanent secretariat for the Conference. The Conference must become an unavoidable interlocutor in all international initiatives which have an incidence on data protection. It must allow room for discussion and allow concrete suggestions to emerge, in order to better follow up on international initiatives, to harmonise practices and adopt common positions.

25. **Elaboration of an International Convention and other global instruments**: in the Declaration of Montreux (2005), the Data Protection and Privacy Commissioners called for the development of a universal Convention for Data Protection. This initiative must be supported by DPAs with the competent institutions, with due respect for their institutional position and for the necessary pre-requirements for national coordination, if applicable. Within this framework, DPAs should endeavour to promote this initiative in their respective spheres of influence, in particular within the regional organisations or linguistic zones to which they belong. The need for global solutions respecting privacy and data protection may arise in specific sectors (e.g. internet governance, financial transactions, air transport) and must then be addressed by DPAs with all appropriate means.

26. **Involvement of other stakeholders (Civil Society, NGOs etc)**: other stakeholders of data protection and privacy are currently active, both nationally and internationally, at different levels and in various sectors. Such organisations may act as strategic partners and contribute substantially to DPAs becoming more effective. Cooperation with other appropriate stakeholders should therefore be encouraged or even actively developed.

IV – TOWARDS A NEW COMMUNICATION STRATEGY

27. Communication is a key condition for making data protection more effective. A message which is not received and understood may just as well not exist. An opinion or decision which is not accessible will have limited impact and may possibly not be worth the efforts invested in developing it.

A – We urgently need to develop and implement a new communication strategy, both at the national and the international levels

28. **Communication as an objective.** Much better communication with the public must be a leading objective for all DPAs. It is not acceptable that in some countries where the right to data protection is a constitutional right, just as freedom of movement or freedom of the press, the vast majority of our fellow citizens have absolutely no awareness about such rights or their importance. It is even less acceptable where there are even negative attitudes towards data protection.

29. We must initiate powerful and long term awareness raising campaigns aimed at informing individuals on the existence and the content of their rights. The effects of these actions need to be measured. Two specific targets must be aimed at:

    - National and local elected representatives, who have a specific responsibility in this matter and whose level of information should be improved,
    - Young people who show little interest in these questions as they are so used to using new technologies. We must act in the educational field as soon as possible.

30. **Communication as a powerful lever**. It is important and urgent that our DPAs are granted better means of action and that they are ensured recognition at the international level. Public confidence and support are absolutely essential. Data protection must be made more concrete. It is only those organisations which communicate, usually through the media, in ways which are **meaningful, accessible and relevant** to the public at large, which will gain the necessary power to influence public opinion, and thus be heard and taken seriously by the States and the international community. Meeting this condition is necessary to obtain these indispensable means of action.

31. This implies that we all use communication professionals in our authorities, and that communication messages are as consistent as possible across all DPAs.

B – An interesting communication message would be to draw a parallel between the preservation of individual liberties and the preservation of the environment

32. One may not act with impunity with regard to environmental issues. In the same way, we must be extremely careful in the data protection field with any uncontrolled technological evolution or with any law that may be enacted without a clear vision of the risks at stake. We then run the risk that our “capital” in terms of liberties and of identity is reduced or even destroyed. And it will not be renewed, precisely because technological innovation is irreversible.

33. Privacy and data protection may in fact be just as precious as the air we breathe. Both are invisible, but the effects may be equally disastrous, when they are no longer available.

V - PROGRAM OF FOLLOW-UP ACTIVITIES

34. The discussion of this initiative at the closed session of the International Conference of Data Protection and Privacy Commissioners in London should be seen as a first step towards a growing consensus about the need to act and to develop means to communicate better and make data protection more effective.

35. DPAs supporting this initiative undertake to further develop and where necessary be responsible for a number of joint activities, to be reported on and followed up at the next conference in Montreal, such as:
    - Workshop on strategic issues: conditions to make DPAs more effective; possible development of "principles of good supervision" in data protection; information on best practices (commissioners and strategic staff); reflection on the development of an international convention;
    - Workshop on communication: available expertise in communication on data protection (e.g. campaigns, opinion research); developing a joint message and effective tools for spreading it (communication professionals);
    - Workshop on enforcement: available expertise in monitoring and ensuring compliance; effective means for inspection (including audits) and intervention (commissioners and enforcement staff);
    - Workshop on internal organisation: recent experience with organisational change; projects to improve efficiency and effectiveness (commissioners and organisation staff);
    - Any other activities considered relevant for this initiative.