



Convention 108: from a European reality to a global treaty

Council of Europe International Conference

Strasbourg, 17 June 2016

Giovanni Buttarelli

European Data Protection Supervisor

Dear participants, dear colleagues,

I am very pleased that you have given me this opportunity to contribute to this important Council of Europe Conference which takes place at a crucial moment for the future of the Convention 108/9181. I really hope that today's debate contributes to reinforce its principles all over the world.

I will start with a reference to an issue that is currently very popular, the EU-U.S. Privacy Shield on which my institution has adopted a recent Opinion following the one by Article 29 Working Party.

The first draft adequacy decision was the result of a couple of intense years of negotiation between both parties. And I have to say that if both had been parties to Convention 108, the whole process would probably have been much smoother.

This is just one example of how important the global dimension of Convention 108 is, not only for individuals, who expect to be protected across borders, but also for companies which have to work in an era where data flows, unlike laws, do not respect national boundaries.

But I would like to outline a key feature of both the EU legal framework and Convention 108: they apply **without discrimination** on the basis of nationality or residence.

This principle of non-discrimination is one of our core values. Now, more than ever, we need to defend it and apply it. It is also in light of this principle that the universality of Convention 108 becomes important.

I would also like to highlight the **revolutionary scope** of these two instruments. The General Data Protection Regulation (GDPR) will now clearly apply where organisations or companies not established in the EU offer goods and services to individuals in the EU or monitor their behaviour.

As regards the Convention, one of its best assets is its *material* scope. Unlike the EU Charter of Fundamental Rights and the GDPR, which are limited by the transfer of competences to the EU by its Member States, **the Convention does not contain a general exemption for national security**. This provides a solid framework of fundamental principles for all parties to the Convention, independently of the GDPR and the law enforcement Directive, which should be retained.

The Council of Europe and the EU have led the way in renewing the rulebook for a new generation. They have taken significant and brave steps and this progress should not be reversed in any way. The new instruments should provide increased legal certainty for both individuals and organisations processing data. They have been adapted with the digital environment in mind and include greater protection for the individual such as a stronger right to object, with the burden of proof on the controller and a general obligation for data breach notifications. The provisions on automated processing or profiling are also remarkable. As a Supervisory authority of the EU institutions including as from next year Europol, **the importance placed on independent supervision** is particularly gratifying.

According to the newspaper headlines, the big question is whether companies in the private sector are ready for these changes. But as I said at the last Spring Conference of Privacy and Data Protection Commissioners, an equally big question from me is – **are we ready?** Are EU Member States and the current and future parties to the Convention sufficiently aware, equipped and cooperative to face this brave new world?

Like all of you, my small institution has been bombarded this year with requests from industry groups, NGOs and think tanks for insights into what will happen next. How will the regulatory reforms be implemented in practice? Will we all be able to provide timely and

relevant guidance on the areas of data protection which, despite the changes this year, are less than 100% certain?

In the EU, data protection authorities (DPAs) have been given greater powers, and we all know that with more power comes more responsibility. Something similar will happen for DPAs in the European Economic Area and for DPAs of those countries party to a modernised Convention 108, notwithstanding the outcome of the EU referendum in the UK.

I would also like to stress the importance of the **Cybercrime Convention**. First of all, to ensure its good functioning and consistency, the parties to the Budapest Convention, which is about sharing data, should be encouraged to be parties to Convention 108.

While 49 countries signed the Budapest Convention, 48 countries have ratified Convention 108 and more are to come very soon. I believe that a synergy between the two conventions is to be found. For example, the so called "Cloud Evidence group" set up within the Cyber Convention Committee met some weeks ago here in Strasbourg to discuss the interaction between data protection regulation and the cross border investigation instruments, such as the Budapest Convention.

The discussion revealed that data protection and cross border criminal investigations are not two conflicting frameworks. On the contrary, data protection instruments, such as Convention 108 and the new GDPR aim to establish a coherent and consistent framework to guide the processing of personal data, with a particular focus on the cross border processing of data. In this context, the Budapest Convention may and should take advantage of data protection rules to better identify the person in charge of the data, the different processing at stake, and the different transfers taking place.

Of course, Convention 108 and the Data Protection Directive have been revised or are being revised, to deal with the challenges of the cross border digital world. Therefore, the Budapest Convention might also go through the same process, and adapt accordingly. However, it would be foolish to think that both exercises could be done without giving consideration to both the privacy and data protection aspects, and to better and more efficient international cooperation in terms of cybercrime and access to digital information.

I have been arguing that one of the biggest policy and legal innovations in the GDPR is the notion of **accountability**, which requires controllers to comply with and to demonstrate compliance with the new rules. The notion of accountability will soon spread outside the EU.

However, as many have said in the last few years, the most significant, practical innovation in the EU is the introduction of serious **sanctioning powers**. The potential of fines of up to 4% of annual global revenue – this is the provision which should make an impact in executive board rooms around the world. It should make an impact – but whether it *will* make an impact depends on the way we, as DPAs, implement it.

Taken together three factors create a potentially robust regime for safeguarding digital rights:

- accountability
- enhanced powers of independent authorities and
- cooperation between those authorities.

These factors are present also in the draft text of a modernised Convention 108.

The success of a modernised Convention 108 and the GDPR, depends more than anything else, on our integrity and on our passion for the rights of individuals in the digital age.

I'm following the debate in Strasbourg and I see how difficult it is in its last mile, as it was the case for the GDPR.

By using Star Wars language, allow me to say that it takes strength to resist the dark side. Make the principles of Convention 108 digital, don't water down them.

May the force be with you.

Thank you for listening.