
*Hitting the ground running: How regulators and businesses can really put data protection accountability into practice*

*Keynote speech at European Data Protection Days (EDPD) Conference*

Berlin, 15 May 2017

*Giovanni Buttarelli*

*European Data Protection Supervisor*

Ladies and gentlemen,

First of all, I would like to thank the organizers for the invitation to this Conference on the very pertinent topic of accountability.

It is a particular privilege to be opening this year's conference, because we stand at a particular moment in time. The world-wide ransomware assault of few days ago has already crippled more than 200.000 victims in at least 150 countries. Cybersecurity, privacy and security challenges are growing around the world. It is therefore a high-time where the world of data protection is looking forward to provide more security and restore trust by setting world-wide standards, also with accountability.

Yes, we are almost exactly one year away from full entry into application of the General data protection regulation in the EU and with it we will see more legal certainty in an increasingly globalised environment.

Soon controllers, as well as data protection authorities in the EU will be stepping into a new - for sure exciting - era, the era of GDPR.

In particular, one of the key new features that GPDR will bring into legal reality is the concept of accountability.

Accountability really constitutes a new key principle of the GDPR.

As privacy and data protection professionals, you probably witnessed the discussions on how to install this principle in binding, directly applicable law.

From the early work and reflections conducted within workshops (into which the EDPS took an active role) in Dublin, Madrid, Warsaw and Brussels, it took a lot of work to bring us to the mature accountability concept that we now have in the Regulation today.

In July 2010, the Article 29 Working Party has highlighted in its Opinion n. 3/2010 that EU data protection principles are often insufficiently reflected in concrete measures, and that there is a strong need to move from theory to practice.

Now, the GDPR includes a direct reference to the "accountability principle" in Article 5.2 and Article 24, which requires the implementation by controllers of appropriate technical and organisational measures.

Controllers will have to demonstrate compliance with data protection principles, and demonstrate responsibility by adopting appropriate business models. Indeed, with less formalities comes greater responsibilities.

Processors will also have to uphold this principle: Companies processing personal data will have robust risk management and demonstrate in a transparent manner that all necessary measures have been put in place.

I should stress here that accountability is not the Trojan horse to legal requirements: it comes in addition to these requirements. Of course, you always need to have legitimate grounds prior to processing personal data.

Accountability is, at the same time, an opportunity: If properly implemented, it is an incredible tool to implement tailor-made and personalized measures adopted to the specificities of each organisations, in order to make data protection more effective.

While the clock is ticking closer and closer to the deadline of entry into force of the Regulation, the main question for companies now is: how will data protection authorities implement accountability in practice?

We could also put it this way: are EU DPAs embarking on an adventure in uncharted territory, such as the one of the USS enterprise from the Star Trek TV series, namely: "*to explore strange new worlds, to seek out new life and new civilizations, to boldly go where no man has gone before*"?

Though we will enter the new era of GDPR, I would like to stress that unlike the USS enterprise from Star Trek, we will not step into the unknown.

EU DPAs are already equipped with the right tools to check that accountability works in practice.

For example we apply the principle of accountability, already now, to the European Union institutions, bodies, agencies and offices that we supervise as EDPS.

In 2016, we launched a project called the "accountability initiative" aiming to bring about a culture change in EU institutions based on the principle of accountability.

It began with an internal exercise among our own staff led by the DPO in EDPS. We then rolled it out, among others, in the CJEU, the European Central Bank, the Council of the EU, the European Parliament and the Fundamental Rights Agency.

This proactive approach is necessary because the concept of accountability - now put at the heart of the data protection reform with the GDPR - goes beyond compliance with the rules, it implies a cultural change from inside organisations.

Clearly, this shows that accountability relies greatly on the level of commitment from the management of each organisation.

We at the EDPS also have developed our own accountability questionnaire and template for the controllers under our supervision. We are willing to make it available to all stakeholders who can benefit from the know-how we developed.

Today, we can see as an amusing paradox the fact that some companies which were strongly against the GDPR are now asking for very detailed guidance. This is a first good sign towards the right path - shifting cultures by educating and training controllers.

Of course, the WP29 has set up an Action Plan and has begun intensive work on issuing GDPR-related Guidance for controllers and processors, in order to ensure more clarity and more predictability.

On 13 December 2016, three guidelines on GDPR topics were finalised on:

- the right to Data Portability;
- Data Protection Officers (DPO); and
- the Lead Supervisory Authority.

The EDPS is fully involved in the WP29's Key provision subgroup and in particular in the work on the DPOs Guidelines.

It is interesting to see that the DPO guidelines underline the fact that even before the adoption of the GDPR, it was said that "the DPO is a cornerstone of accountability".

It is true that DPOs will play a key role in accountability.

This is because they facilitate compliance through the implementation of accountability tools (such as facilitating -or carrying out- data protection impact assessments and audits), and because they act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).

More than ever DPAs in the EU are very keen to delivering sound, proper and meaningful GDPR guidance to help companies with the GDPR implementation. However, as DPAs in the EU have already a lot on their plate and as their resources cannot be dedicated entirely towards this only objective, it would be reasonable to expect gradual Guidance releases over time.

Accountability is essentially a practical principle.

For instance, it may imply: up-to-date documentation; registers for international

transfers including the legal basis and the instrument used; and records of where there has been an exception to the rights of information or the right of access (this is relevant to checking compliance when we conduct and inspection or when we have to carry out "indirect access" in the context of a complaint).

We as Privacy and Data Protection Commissioners around the world definitely need to take a sound, pragmatic approach.

For DPAs, this means that they should seek to play a responsible role as supervisors. This means that DPAs will be less prescriptive, but will be increasingly selective to remain effective.

What does having a pragmatic approach mean in practice?

For example, as regards documentation obligations, it was not the spirit of the GDPR to ask controllers and processors to each and every detail of their processing.

A reasonable approach for documentation should be to ask to controllers to focus more on what is essential. In this regard, we could make use of categories to simplify the documentation obligations.

I was in Washington DC a few weeks ago, where I met with companies dealing with accountability in a modern way, for example by demonstrating why digital applications design needs ethics embedded right from the start.

In many ways, Ethics is the new accountability.

In ancient Roman religion and myth, Janus was the god of beginnings, gates, transitions, time, duality, doorways, passages, and endings.

He is usually depicted as having two faces, since he looks to the future and to the past.

But most importantly, Janus presided over the beginning and ending of conflict, and hence war and peace. The doors of his temple were open in time of war, and the doors were closed to mark the peace.

If I may dare this comparison, I would be tempted to say that accountability is, in many ways, not so different from Janus: it has two sides which have to be well balanced and are inseparable.

One side of accountability is that controllers now are free from heavy formalities and have more leeway about how to implement internal measures to ensure compliance with data protection rules. However, this side goes necessarily along with the other side of accountability, which is proper enforcement and supervision by the competent data protection authorities.

In fact, the GDPR moved the cursor from a priori supervision to a posteriori supervision.

So if controllers want to keep the doors of the accountability temple closed -in order to mark their peace with DPAs- they know that they will have to put in place and be able to demonstrate measures that are really meaningful and effective.

As in many other areas, here comes again the need to have good DPAs cooperation mechanisms into place. Fortunately DPAs in the EU and the EEA are able to cooperate amongst themselves as well as with other Privacy and Data Protection Commissioners outside the European Union to develop together flexible guidance, to share best practice and to cooperate on enforcement.

We shouldn't underestimate potential challenges linked with implementing accountability in practice.

For example, how should we as DPAs prepare ourselves to respect and verify implementation of accountability?

Companies implementing proper accountability measures are allocating significant resources in time, money and people in order to ensure compliance.

However, do we as DPAs have the necessary expertise to evaluate an accountability plan? Such evaluation might, in practice, prove more difficult than performing a simple legal grounds check, as DPAs now might need to understand far better how the company works from the inside to be able to appreciate if the measures put in place are meaningful.

This takes us back to the necessary dialogue that business and data protection authorities should have in order to make both worlds conversant.

We might also bump into potential issues around the question of scalability. In practice, how are companies and data controllers -but also DPAs- prepared to graduate accountability measures depending on the size of their business or the risk of their data processing?

DPAs should be aware of these challenges but are at the same time ready to find practical and workable solutions in order to overcome them.

Ladies and gentlemen, let me conclude briefly by saying that in order to be a success, the new accountability framework will truly rely on the level of commitment of both organisations leaders and data protection officers.

This means that data protection officers must be granted with enough resources and support to be able to perform their duties.

I want to believe that we are heading towards a better world for data protection, as there are encouraging signs that more and more countries around the world are seeing the big picture, with 121 countries now having adopted or negotiating data protection and privacy laws.

However, we can also see contradictory evolutions, for example in the field of Big Data, where there are trends towards more coercive uses and more behaviour analytics.

In order to deal with accountability, companies as well as DPAs need more flexibility. DPAs must favour proactive, pragmatic and solution-oriented approaches.

Finally, I would like to quote John Wooden, a famous American basketball coach, by saying that we shouldn't mistake activity with achievement.

All our actions, especially in the field of accountability, should be aimed to a goal, which is to achieve better data protection.

I want to thank you all warmly for your attention and to invite you to take full part in this conference.