The accountability principle in the new GDPR

Speech at the European Court of Justice, Luxembourg, 30 September 2016

Giovanni Buttarelli

A new chapter for EU data protection

Europe has opened a new chapter for EU data protection in 2015. After almost four years of intense negotiation and public debate, the General Data Protection Regulation - or "GDPR"- was adopted in April 2016. We are now on track to change data protection in Europe for the next generation.

To do that, we need to find new ways for applying data protection principles to the latest technologies. Think of big data, including its ethical dimension in health for example,

the internet of things, cloud computing, artificial intelligence, drones or robotics. Holding true to data protection principles at the same time as embracing the benefits of technology means less prescriptive rules. It means, instead, more accountability for how personal information is treated. That means asking the legislators to do less - and asking the controllers and independent regulators to do more.

The new rules give us a unique opportunity to strengthen data subjects' rights and the accountability of data controllers in public and private sectors. This means better protecting fundamental rights and freedoms in a modernised way; to lead by example around the world with global partnerships in the interests of the individual. Our Strategy 2015-2019 includes the objective of opening of a new chapter for EU data protection. It is our vision to help

the EU lead by example in the global dialogue on data protection and privacy in the digital age.

Let me note that EU bodies must be fully accountable for how they process personal information. To demonstrate exemplary leadership, we must be beyond reproach. That's why EU bodies should lead the way in demonstrating accountability in practice.

****

EU bodies should lead the way

The new General Data Protection Regulation -the “GDPR"- will include a direct reference to the “accountability principle” in its Article 5(2) and will require under Article 24 the implementation by controllers of appropriate technical and organisational measures to ensure and demonstrate compliance. Some of these measures are further described in Chapter IV of the GDPR. Provisions in

this chapter include accountability instruments like appropriate data protection policies, data protection by privacy by design and by default, IT security risk management, data breach notifications, data protection impact assessments, prior consultations and Data Protection Officers.

Regulation 45/2001, the data protection framework specifically applicable to EU institutions, will be revised this year to align it with the rules of the new GDPR. These revised rules will most likely impose the specific obligation of accountability on the EU bodies as a compliance requirement in itself.

****

What does "accountability" stand for?

So what should we understand by "accountability"? Let me start by saying what it is *not*: It's not a Trojan horse for

introducing more red tape. I have argued forcefully for the GDPR to reduce administrative burdens. And I am certainly not going to advocate anything that bureaucratises data protection for EU bodies as a result of it.

So what *does* the principle of accountability stand for? It helps in moving data protection from theory to practice. Accountability goes beyond compliance with the rules - it implies culture change. As such, accountability needs to be embedded in the organisation. As controllers, EU bodies are accountable when they are able to do the following key things:

1. Firstly, establish transparent internal data protection and privacy policies. These need to be approved and actively endorsed by the highest level of the organisation's management.

2. Secondly, put in place appropriate and effective internal processes and tools to implement these policies. This ensures that data protection principles and obligations are complied with and that individuals are adequately protected from risks stemming from the processing of their personal data.

3. Thirdly, informing and training all people in the organisation on how to implement these policies.

4. Fourthly, responsibility lies at the highest level for monitoring and assessing the effectiveness of this implementation. Out of this monitoring and measuring, the organisation needs to be able to demonstrate to external stakeholders and supervisory authorities the quality of the implementation.

5. Fifth and last point: The organisation need to put in place procedures for redressing poor compliance and data breaches.

****

Accountability is not new to EU institutions

In many ways, accountability is not new to EU institutions. Whilst Regulation 45/2001 does not specifically articulate the principle of accountability, it is, for example, implicit in the already existing requirement under Article 4(2) on the controller to ensure that the requirement of data quality is complied with.

Let me give you another example. In our 2011 Survey measuring compliance of EU institutions with data protection rules, we recommended that, in addition to a register for processing operations that have been notified to the Data Protection Officer or the EDPS, EU bodies should

have an *inventory* of all processing operations, including those at planning stage. Some reacted by suggesting that the EDPS was asking for something going beyond the scope of Regulation 45/2001. However, such an inventory gives the Data Protection Officer and the hierarchy a holistic view of the organisation's processing operations and facilitates the identification of risks. It is thus a pre-requisite for the controller being in control on data protection. Not surprisingly, having an inventory has become an accepted standard for EU institutions.

However, whilst the legal responsibility for compliance has always been with the controller, this has so far often produced mainly formal results. For example, a mere notification sent to the Data Protection Officer.

****

GDPR means a quantum shift

With the GDPR comes a quantum shift in emphasis: controllers are responsible – not Data Protection Authorities or Data Protection Officers.

As a practical consequence, EU bodies as controllers need to be proactive – at all levels:

- For top management, the message is that data protection concerns *you personally*. It's the tone at the top that matters. Data protection is not another formality that can be delegated to "controllers in practice" or to your Data Protection Officer.

  Regular reporting on data protection is key and certainly a step in the right direction. But have you allocated data protection responsibility and resources where they belong? What have you personally done to

encourage data protection initiatives? Is your institution prepared for future privacy challenges?

And if the answer to all of this is a resounding "yes" - *are you really sure*?!

Consider that with a general public that is more and more data protection aware, accountability needs to also be embedded in your institution's actions regarding ethics and social responsibility.

- For high level management, being proactive means that you ensure that the Data Protection Officer and any Data Protection Coordinator are involved in the early stages of any policy development. Seek regular contact with them and update them and top level management on the state-of-play regarding your projects. Bring data protection by design and data protection by default to life in what you develop - and

talk about it, including to the top level. Note that they will expect and encourage you to do so! Regard data protection as another building block of your risk management responsibilities. Keep in mind that, for example, public procurement without a green light from the Data Protection Officer can cause personal liability on top of reputational damage.

- At staff level, keep in mind that your Data Protection Officer and any Data Protection Coordinator must be on board at the early stage of any policy, process and system developments. Make sure you receive adequate information and support from them and, where required, additional training on data protection issues. Proactively inform your hierarchy about data protection aspects of what you do - they will have encouraged you to do so!

Why is this significant?

- *Proactive* data protection means that decisions have to be taken in advance: There will be an incentive to embed the management of data protection and to make it part of forward planning and risk management. Think of the need to conduct proper public procurement, to avoid liability and to prevent any reputational damage;
- *Effective* data protection that works in practice benefits data subjects. Let me reiterate: To demonstrate exemplary leadership, we, as EU institutions, must be beyond reproach. Because if we are not, know that Article 83 of the GDPR foresees administrative fines for infringing GDPR rules. And in a case where an EU institution breached the rules by

unlawfully transferring health data, the European Court of Justice has already fined them 25.000 Euro.

- These measures complement and animate all controller obligations, existing and new ones.

****

Impact on EDPS supervision

That calls for a word on how EDPS supervision will change - or not. The EDPS will increasingly need to be selective to remain effective. That means

- We will be using inventories of data processing operations. Be prepared to react to our call to "*Show us your books!*";

- We will practice a *strategic* supervision approach, with scalable EDPS control. Admittedly, that is not really new. For example, in our bi-annual Surveys measuring

compliance of EU institutions with data protection rules, we have always grouped EU bodies to make them comparable according to their size, maturity and core business. The same is true for selecting specific EU institutions for on-site inspections, where our decisions are based on a risk analysis;

- The EDPS can no longer rely on notifications to provide a "trigger" for action and a broad overview of processing operations. That increases the need for close cooperation *beyond* Data Protection Officers and Data Protection Coordinators. We will need to step up our awareness raising efforts, for example for staff responsible on behalf of the controller. With data protection going digital, providing guidance on the technical implementation of data protection will become an increasingly important task for the EDPS.

And, where required, we will need to opt for *proactive* enforcement.

******

Why is the EDPS conducting accountability visits *now*?

As mentioned, the new rules are not in force quite yet - but it is already clear what lies ahead in terms of future obligations. Getting ready *now* is ideal timing - as part of risk management, don't leave it until the last minute. That is why we are conducting accountability visits *now*. Starting now also allows you to find tailor-made solutions to meet any specific needs you might have for your institution and its specific context and core business.

******

EDPS leading by example: the EDPS accountability tool

How can the EDPS help you? The EDPS strategy for 2015-2019 commits our institution to “lead by example” in the way EU institutions protect personal data.

In 2015, we initiated a project to develop a framework for greater accountability in data processing. This was applied first of all to the EDPS, as an institution, a manager of financial resources and people - and a *controller*.

A specific tool has been developed to ensure and demonstrate EDPS accountability, to plan and to keep track of related actions. It consists of a set of questions for the Supervisors, the Director, the staff responsible for managing processing operations and our Data Protection Officer.

Let me be clear: I am not trying to sell you just another box-ticking exercise or some sort of quasi-automatic excel sheet. That would not only increase administrative burden, but also the risk of failure to truly embed accountability in the organisation. There is no such thing as culture change by check-list!

Instead, our tool asks *open* questions and gets all organisational levels and areas of activity thinking. Data protection is not sectoral, but interacts with the rest of the organisational structure. Consequently, everybody, including top management, is invited to provide evidence of high level technical and organisational measures to protect personal data and ensure accountability.

The questions relate to data protection measures in the main areas of activity of the organisation. One of the questions all EDPS departments will need to answer is, for

example, how we ensure that all EDPS staff is aware of the data protection guidance given by the EDPS in the form of guidelines and newsletters.

The questions do not go into the detail of these measures, but rather aim at ensuring that the organisation is in control of personal data and their lawful processing. Periodic verification of the accountability status will be synchronised with the review of the EDPS Annual Management Plan and/or the Risk Management Exercise.

The benefits of this internal accountability exercise include a reliable inventory to report on data protection measures and safeguards. It also produces plenty of evidence to ensure ownership and enable choice as well as a comprehensive to-do-list to further improve the accountability status.

I recommend you give this tool a try on your way to implement accountability. Tweak it until it suits any specific needs you might have for your institution and its specific context and core business. I encourage you to find tailor-made solutions - and to let us know about them.

****

Let me conclude by highlighting that the success of the new accountability framework depends more than anything on the commitment of the leaders of organisations - and on the diligence of Data Protection Officers.

Data Protection Officers must have enough support and resources to perform their duties. Consider them as your internal supervisory body. It is their role to advise and recommend on all matters data protection - but they are and remain independent. That means that Data Protection

Officers are *not* the ones to get the accountability job done for you!

But fear not: The EDPS is ready to help equip you in the EU institutions to do this. Today's visit and the tool I introduced you to is only the first step.

To be continued...