Christopher Docksey - Keynote on Accountability

Good morning. I would like to thank the International Conference and Commissioner Besnik Dervishi and his staff for inviting me here today and for their excellent welcome.

10 years ago, on 6 November 2009, this Conference embraced accountability in the **Madrid Resolution** on International Standards for the Protection of Privacy. This marked the culmination of a series of meetings lasting over a year, which started with the idea that international transfers of personal data could be facilitated by accountability. Of course this aspect is still a very important element of BCRs and the CBPR. However accountability was transformed over these discussions from a principle limited to international transfers into a self-standing general principle.

As a result, Article 11 of the **Madrid Resolution** provides (paraphrasing) that the data controller shall actively develop compliance, and be able to demonstrate compliance to data subjects and to regulators.

I would like to use this Keynote to show why this text, adopted, almost exactly ten years ago, is so important, and to discuss what accountability means, and how can it be achieved.

To establish my credentials maybe I should start with my own experience of accountability. As head of the EDPS Secretariat I was both a regulator and the data controller. Of course I made sure that the EDPS was *compliant*, but I had to have a "Eureka" moment, or a "Damascus" moment, to learn that accountability means more than compliance. I was not in the bath like Archimedes, nor on the road to Damascus, like St Paul. I was on the train to Paris to give a talk to CPOs. I read a handbook on the train, which explained what accountability actually entails, and I understood, to my dismay, that we were compliant but not accountable. I actually thought "Uh oh, I hope they don't ask me what *we* are doing to be accountable"! Fortunately, as you know, privacy professionals are caring persons, and I returned safely to Brussels. And then it took over two years to develop our accountability programme.

The meaning of accountability

Not enough people know what the principle of accountability means for delivering privacy and data protection. Richard Thomas tells us it is an amorphous word, a typical Anglo-Saxon word, derived from keeping accounts. Indeed in some languages there is a similar nuance of financial accountability or of paying the bill, for example *Rechenschaftspflicht* in German and *rozliczalność* in Polish. Many languages simply use the word 'responsibility', for example *la responsabilité* in French.

But the word responsibility is too close to compliance on the one hand and to legal liability for non-compliance on the other. Accountability is different.

The key elements of accountability can be found in the terms used in Colombia and Spain: *la responsabilidad proactiva* (Spain) - actively developing compliance – and *la responsabildad demostrada (*Colombia*) – being able to demonstrate compliance.*

Put them together and you have accountability: *la responsibildad proactiva y demostrada:* actively developing, demonstrating, and being able to demonstrate, compliance

In reality, accountability is a term of art - what matters is what accountability *is*, not what its name is. We should remember what Romeo thought about Juliet and her family name: "a rose by any other name would smell as sweet." So if the word for accountability is not very helpful in your language, think of it as a rose: eminently desirable, but supported by sharp thorns.

A**ccountability across the world**

If accountability is a rose, it has been flowering across the whole world. The original **OECD Guidelines** in 1980 include the term 'accountability'. However they use the word only to mean *compliance with legal obligations*.

As I realised on the train to Paris, compliance is different to accountability, simple compliance with legal requirements is not enough. Accountability is a fundamental shift in approach. In effect, it has moved data protection from an *adjective* to a *verb*. What we had before was an adjective, a *definition* of who was the *person responsible* Now we have a *verb*, an *activity*: what is the responsible person *doing*?

The first legislation on accountability in this sense was the **Canadian PIPEDA** in 2000. It was followed by the **APEC Privacy Framework 2005**, which is implemented by an accountability mechanism in the APEC **Cross Border Privacy Rules** ('CBPR').

Things really started moving from 2008-2009 onwards. In the **Global Accountability Dialogue**, a series of meetings also known as the ***Galway Project***, regulators, organisations and individuals through civil society co-operated and exchanged ideas. As a result, the accountability principle was adopted in the **Madrid Resolution in 2009**, and in the Article 29 Working Party **Opinion on Accountability in 2010.** In this Opinion the Working Party specifically asked the Commission to include an accountability clause in the future GDPR, and its inclusion in the GDPR represents a significant policy success for EU regulators.

In 2012 Canada took the lead again: three Canadian Commissioners provided guidance on **Getting Accountability Right with a Privacy Management Programme.** This was a crucial step: without guidance, most organisations have no idea what to do in practice to be accountable.

From then on guidance on accountability was developed by regulators across the world: in 2013 the Best Practice Guide in **Hong Kong**, in 2015 the Guide for the Implementation of the Principle of Accountability in **Colombia** and the Privacy Management Framework in **Australia**, and in 2018 the Privacy Accountability and Compliance Framework in the **Philippines** and the Model AI Governance Framework in **Singapore**.

Over the same period, an increasing number of countries and international organisations adopted accountability into their national laws. **Mexico** adopted accountability in the **2010** Law and explained it in the **2011** Regulations. The **OECD** updated their **Guidelines** in 2013, to include a new Part Three on Implementing Accountability, and in 2016 the **EU**

enshrined the accountability principle in **Article 24 GDPR**. Peter Hustinx says that Article 24 is his favourite article of the GDPR, and is "arguably the most central provision of the Regulation."

In 2017, **Guernsey** - which has an existing "adequacy" finding from the EU - updated its data protection law in line with the GDPR, including the accountability principle. There is a lesson in this for the other existing "adequacy" countries, which would be well advised to include accountability in their updates too.

Perhaps most importantly in this list, in 2018 the accountability principle was enshrined by the Council of Europe in Article 10 of **Modernised Convention 108**.

In Africa, The Ghana Commissioner, Patricia Adusei-Poku, has stressed at this conference that African regulators are looking to accountability and not merely compliance. And this year, **Brazil** adopted its GDPL, which also specifically includes the principle of accountability.

This brief history illustrates two important points:

First, accountability is a **global standard.** Colleagues across the world are used to the EU telling them that we are the "gold standard", the "bees knees", and everyone should respectfully listen to us. But we can't say this about accountability. You can see from the timeline that the GDPR came late to the party. We are learning too.

Second, accountability needs both legislation and explanation. It must be in the law - accountability is not self-regulation - and it has to be backed up by effective guidance.

Marty Abrams has blogged that "the basic principle of accountability must be embraced by law with regulators able to generate enforceable guidance related to the principle".

The need to talk about accountability

We need to talk about accountability today because there is a lot to be done. The **GPEN 2018 Data Sweep** looked at how well organisations have implemented the core concepts of accountability into their own internal privacy policies and programmes. It concluded that "organisations should be doing more to achieve privacy accountability". Similarly the **IAPP / EY 2018 report** found that only 32% of organisations considered their program "mature" and noted that 56 % of organisations subject to the GDPR said they are *far from compliance* or will *never* comply.

Accountability can help if it is seen as part of the *solution*, not as part of the problem. The new data protection legislation is invariably criticised as a step too far, imposing onerous obligations and procedures, and so on. But once controllers have understood what it is to be accountable, they will understand the need for the rest.

The road to accountability

One ***pragmatic*** way of understanding accountability is to see it as a **toolbox, full of useful tools.** If we take the GDPR as an example, we can see a number of these accountability mechanisms. They are not merely legal requirements, they also represent best practice:

- privacy by design and privacy by default
- records of processing activities
- security measures and data breach notification procedures
- DPO/CPO
- DPIA /PIA
- codes of conduct
- certification

Too many people think that accountability, and these accountability mechanisms in the tool box, represent yet more legal obligations. However we should see them as *helpful tools* rather than as *extra obligations*, as part of the *solution* rather than the *problem.* And the accountable organisation that uses these tools will find that it has carried out the core of its various legal obligations.

Another way of looking at accountability is as a ***philosophy*****: of being a responsible and ethical steward of personal information.** There are various roads to enlightenment, to saying "Aha! I understand!" If you remember, I had my "Aha!" moment on the train to Paris.

It can come to **top management** if they receive an effective message. Many senior managers realise that privacy, although it is an extra burden, is something that has to be done. **Tim Cook** was like that. A few years ago he was at the same meeting as Giovanni Buttarelli. He invited Giovanni to a short 15 minute meeting and asked him to explain "all this privacy stuff". Giovanni responded by asking him whether he knew the name of his CPO. And they went on from there. Giovanni came out of that meeting over an hour later, and Tim Cook had his "Aha! moment.

The path to enlightenment can also come from **team members**. Maybe by reminding managers that they are processing the personal information of fellow human beings. In **Acxiom**, the analytics team developed a model of '10,000 audience propensities', which included scores for sensitive personal information such as 'erectile dysfunction' and 'vaginal itch'. The leadership team was discussing whether the use of such scores would be too invasive, when one member of the team announced that she would be able to read the actual scores on these sensitive topics for each of the individuals in the room. Once confronted with this very personal information, the leadership team had their "Aha!" moment and understood that these types of scores were 'too sensitive' to be made available as a product to customers.

This story shows how important colleagues can be for raising awareness, and it reminds us that modern data processing can be very, very personal, and that managers need to take it very, very personally.

How to implement the principle of accountability

In 2012, the Canadian Commissioners said that accountability was the "first" among the fair information principles. Why the first? Because it is "the means by which organisations are expected to give life to the rest of the data protection rules".

In 2009, the *Galway Project* identified five 'common elements' of accountability:

1. Organisation commitment to accountability and adoption of internal policies
2. Mechanisms to put privacy policies into effect, including tools, training and education
3. Systems for internal, ongoing oversight and assurance reviews and external verification
4. Transparency and mechanisms for individual participation
5. Means for remediation and external enforcement

I would like to concentrate on four key elements of accountability today.

First and foremost, **organisations must take responsibility** for the personal data that they handle. This starts with ensuring top management commitment, taking data protection seriously, being honest, and managing risks. Top management must then ensure that managers and colleagues *at all levels* have to give their support - otherwise a fine-sounding privacy policy will be a hollow shell.

Second, once there is that commitment, it is time to adopt a **Privacy Management Program** (PMP). It is not necessary to do everything at once, one can prioritise and handle the issues step by step. Accountability is a **process,** a responsibility that requires constant care and attention.

Third, the organisation has to have a **privacy professional, the DPO or CPO**, the person or the team who will assure internal implementation of the PMP. In its 2010 Opinion on Accountability, the Article 29 Working Party stressed that the DPO is the 'cornerstone of accountability'. This year, in the **Stockholm Declaration**, the Nordic data protection authorities recognised the importance of accountability and committed themselves to help ensure GDPR compliance by supporting DPOs in their important tasks.

Finally, I would stress the need to ensure the **transparency** of the measures in the PMP, for data subjects, regulators and the public. Transparency goes to the heart of the concept of accountability. Sometimes it is **not the processing that is the problem so much as the lack of transparency to users.** For example, if Google, Amazon, Apple and Facebook had announced they wanted to make recordings of their smart assistants, and to use human beings to check those recordings for quality purposes; if they had set out a clear framework of what they wanted to do, surrounded by safeguards, and had called for volunteers: then we would not have had the scandals this summer, with newspaper articles on "Why are you snooping on me"? and "Alexa, are you invading my privacy?"

The advantages of accountability

Accountability offers clear benefits to both organisations processing personal information and to their regulators.

For **regulators**, I would underline three reasons to encourage organisations to be accountable.

First, **demonstrated accountability can satisfy the due diligence obligation** of the regulator. Under accountability laws, the first thing the regulator can do is ask to see the accountability records. These records, or their absence, make it possible to distinguish between accountable organisations and organisations that have no clear overview of their processing activities, thus **enabling the regulator to prioritise its investigatory work** on the latter.

Second, **accountability minimises over-reporting of data breaches.** An accountable organisation will know when to notify and, more important, when *not* to notify. There is a huge difference between the percentage of data breaches that people *assume* should be notified (100%), and the percentage that actually *have to be* notified after good incident risk preparation and assessment (10%). Such knowledge represents a huge saving of effort for both regulators and organisations.

Third, accountability can work as a bridge between jurisdictions. Andrea Jelinek has noted that accountability can help bridge jurisdictional and legal differences by creating interoperability. It can facilitate transnational investigations by providing a more uniform environment, based on mutually agreed or commonly accepted privacy and implementation standards.

Equally it can also be a bridge for organisations: Paul Breitbart says it works like an electric converter plug, which fits in each jurisdiction, even if the exact legal requirements are different.

However, as many regulators already know, **this means a new type of work for regulators**. They have to invest resources in accountability, be creative, and think how to help controllers understand. Many regulators of all sizes have already identified where support is needed. For example, in Guernsey the regulator organises popular "drop-in" sessions for controllers every other Wednesday morning. In Madrid the Spanish regulator has developed the Facilita software tool to help small and medium size enterprises deliver an adequate level of data protection. On this ten year anniversary of the Madrid Resolution, it is apppopriate that last Monday evening the staff of the Spanish DPA won this Conference's Accountability award for developing this tool.

So regulators have a lot of accountability work to do, to provide leadership, support and guidance.

For **organisations**, I would underline four reasons to be accountable.

First, accountability **prepares for the known unknowns** - Subject Access Requests, data breaches, complaints and investigations. The GPEN Data Sweep last year shows that there is a real need here, because a number of organisations had no processes in place to deal with the complaints and queries by data subjects, nor were they equipped to handle data security incidents appropriately.

Second, accountability helps **when the regulator calls**, because there will be a documented privacy policy to show the regulator. **Bojana Bellamy** will tell you that regulators should take demonstrated accountability into account when carrying out investigations and enforcement. You can see this approach in the Singapore regulator's **Model AI Governance Framework, which states** that, whilst adopting the voluntary Framework will not absolve organisations from compliance, it will help to demonstrate that they had implemented the necessary accountability-based practices. Indeed, legislation could even provide a Safe Harbor one day, as can be seen in the AIF Model Accountability Law, which provides that an accountable organisation that has satisfied the requirements of a PIA or a code of conduct should not be subject to civil penalties.

Third, accountability can provide a **competitive advantage.** A strong privacy policy on the website means consumer trust and a strong reputation. The EDPS has argued strongly that accountable firms should gain a competitive advantage from being fully accountable.

Fourth, accountability provides a **methodology for dealing with the game-changer of Artificial Intelligence**. The accountability toolbox is already available, it provides the tools to respect privacy and to develop AI at the same time. For example, **risk assessment** (an automated decision-making with legal or significant effects on data subjects will always trigger a DPIA under the GDPR), **privacy by design and privacy by default** (ensuring that meaningful human review will be designed in from the outset), and **transparency** (to provide information on the values that underpin automated decisions).

Accountability when things go wrong

Finally I should mention the disadvantages of not being accountable when things go wrong. The thorns on the stem of the rose. We should have no illusions, whatever can go wrong will go wrong.

For most controllers, who want to do the right thing, accountability means preparing in advance, organising security, and putting all the necessary procedures into place. An accountable organisation, which has put in place robust programmes, is in a good place when things go wrong and the regulator calls.

However if you fail to plan, you plan to fail, and when something goes wrong, you will be sanctioned, even fined: as Marriott and British Airways are finding out this year, courtesy of the ICO.

Indeed, administrative fines should and will be used to support accountability. For example, the GDPR uses the same risk-based approach for both accountability and for fines: "risks of varying likelihood and severity for the rights and freedoms of natural persons." If you are accountable, you will have taken these risks into account; if not, you risk being fined.

Moreover the GDPR specifies that fines may be imposed for failure to implement the accountability mechanisms in the Toolbox. It is a mistake to assume that accountability

tools are too abstract for fines: on 27 June 2019 the Romanian regulator fined UniCredit Bank the equivalent of € 130,000 for failure to implement Privacy by Design.

Fines have a particular role for organisations that resist compliance or that merely pretend to be accountable. An organisation is not accountable if it hides behind consent, and says one thing in its PR and its privacy policy, but does something else in the research lab and on the website. Accountability is not about treating the risk of noncompliance as a business risk to be factored into turnover forecasts. Such organisations can be faced with three consequences in particular.

First, fines have been calibrated for these organisations to be horizontal in scope and potentially very high. For example in the EU the GDPR has powerful, competition-level fines, first imposed by the CNIL this year against Google. Regulators in Germany have recently developed a model on fines set on the high side so as to be particularly dissuasive.

Second, in addition to fines, such organisations can be subjected to **enforced accountability.** For example, the FTC has recently imposed significant fines on Equifax ($575 mn) and Facebook ($5 bn). We have learned that the members of the FTC disagree whether these high fines were sufficient and whether other remedies should have been imposed to address incentives and the business model itself. However it should be noted that in these two cases the FTC also imposed **accountability mechanisms**: the Equifax Board must obtain annual certification that it is complying with the FTC order, and the Facebook settlement imposes independent accountability mechanisms at all levels - a new independent Privacy Committee at Board level and Compliance Officers at operational level.

Third, research on corporate psychology has shown that even high fines are not as persuasive as **damage to the business**. Companies can absorb even high fines as costs of doing business, but they do care about making profits, and If their reputation suffers, it can harm their sales.

Finally, if an organisation ends up in court, it is increasingly likely that it will be held to account. Courts across the world are becoming more sensitive to enforcing privacy and data protection.

In *Riley v California*, 2014, the **U.S. Supreme Court** warned that "privacy has a cost." In *Puttaswamy v India,* 2017, the **Indian Supreme Court** emphasized that "Privacy is the constitutional core of human dignity". In this ruling the Supreme Court insisted that India should develop a "robust regime" of data protection, including, specifically, accountability, and indeed accountability can be found in Section 11 of the ensuing Indian Data Protection Bill.

In the **EU**, the case law of the **Court of Justice** since *Google Spain*, 2013 has deliberately applied the data protection rules as broadly as possible in order to ensure "effective and complete protection of the persons concerned." This time last year, at the 40th International Conference in Brussels, President Koen Lenaerts said that the Court of Justice is attached to 'high levels of accountability' of individuals that process personal data, in light of the 'central theme' of accountability in the GDPR. It is worth looking at the recent EU rulings on transparency, tracking and consent in *Wirtschaftsakademie*, *Fashion ID* and *Planet 49*. These rulings may well mark a tipping point for the present economic model of private surveillance.

In conclusion, a decade on from Madrid, a lot has been achieved, but there is still much work ahead.

Accountability has been established as a **world-wide principle**, on the move across the globe. I hope we will see more and more legislation on accountability and on increased powers for regulators.

Accountability is, according to Liz Denham, **"crucial, crucial"** for protecting personal data in the digital age. It requires organisations to be responsible, to understand the risks their data processing creates and to mitigate those risks, and it weaves data protection into their cultural and business fabric.

Accountability **empowers regulators**, but they have to work at breathing life into what it means.

Finally, an accountable organisation will develop naturally towards **"Accountability 2.0".** This is about more than avoiding risk to customers. It is **responsive**, creating value for individuals and society as well as for organisations; it is **transparent** about what it is doing, and why, and it is **ethical,** because data controllers are aware they are processing the personal information of fellow human beings.

Looking forward to Accountability 2.0, I would like to conclude with a quote from **Giovanni Buttarelli,** at the International Conference last year:

"Not everything that is legally compliant and technically feasible is morally sustainable".

Thank you.