Anti-fraud investigations and data protection in the EU

Brussels, 5 June 2015

European Anti-Fraud Congress

Giovanni Buttarelli

European Data Protection Supervisor

Ladies and gentlemen,

I would like to first thank the organisers, the European Institute of Fraud Auditors, for inviting me to speak to you today. To kick-off, let me note that it seems quite timely to talk about anti-fraud in multinational organisations. I am delighted to contribute to today's European Anti-Fraud Congress from the perspective of the European Data Protection Supervisor.

As an independent supervisory authority, at the EDPS, we are in charge of monitoring the processing of personal data by the EU institutions and bodies and advising the EU legislator on policies and legislation that affect privacy, including on the General Data Protection Regulation, or *GDPR* in data protection lingo. When advising on the reform of the current data protection rules, the EDPS can **leverage on our extensive expertise as supervisory authority**.

For me, as European Data Protection Supervisor, today is a welcome opportunity to explain the contributions by the EDPS in recent years to discussions on correct application of rules and principles of data protection whilst ensuring transparency of the EU administration.

In March this year, we published our five year strategy, and our intention to raise awareness of data protection rules and principles and how to apply them in specific sectors, in practice and in policymaking, is key.

Anti-fraud is no exception.

I would like to illustrate this by, firstly, outlining how we conduct our supervisory role in the anti-fraud area, the European Anti-Fraud Office. Secondly, I will be referring to **selected opinions and guidelines** issued in the context of anti-fraud measures by EU administration. On that basis, I will then outline some of the **"lessons learned"** and their fruitful effect on **our contribution to the GDPR** beyond the specific domain of anti-fraud.

***

First let me say that the EDPS, like other data protection authorities, is an advisor to the institutions on policies and legal proposals. But we also of course exercise our supervisory **role** in ensuring OLAF operations comply with data protection rules:

- Under Regulation 45/2001, which contains the data protection rules applicable to EU administration, certain "risky" processing operations must be examined by the EDPS before coming into effect. Given their sensitivity, not surprisingly, many areas of OLAF activities have been **prior checked**. In the field of internal and external investigations, we especially looked into aspects connected with due process and the right of defence. This concerns the obligation to provide information to the individual concerned, the right of access, as well as other issues that might affect fundamental rights, such as the confidentiality of communications.

- We have also dealt with **consultations** submitted by OLAF on the application of certain legal provisions to cases that might present practical problems, as in the case of the right of access. These are very practical cases, with OLAF asking for guidance on specific questions that came up in their operational business.

- Furthermore, we have handled a number of **complaints** against OLAF, some of which have resulted in recommendations that have been respected.

- We also conducted on-the-spot **visits and inspections**, in order to verify the state of implementation of data protection obligations in selected cases.

- Last but not least, we're in frequent contact with OLAF - on staff or management level, as the issue at hand requires - discussing both specific cases and general policy directions.

As you see, OLAF is in the end supervised the same way and following the same rules as other EU institutions and bodies, despite the specific nature of its core business.

***

Secondly, next to our cooperation with OLAF, we build on expertise accumulated over the years through the **prior-checking of processing operations notified to the EDPS** by other EU institutions and agencies.

In the following minutes, I'd like to share some specific cases with you, to show what the application of our supervision toolkit looks like in practice, both for OLAF and for other EU Institutions and agencies and which data protection aspects are likely to be relevant in the domain of anti-fraud.

In the area of anti-fraud schemes operated by EU administration, this mostly concerns databases identifying certain entities whose access to EU funding or contracts should be restricted or excluded on the basis of the Financial Regulation.

The main database is the **Early Warning System operated by the European Commission**, but the EDPS has issued opinions also on a number of other, similar, schemes operated by EU Agencies.

Let me illustrate three main "lessons learned" by using a concrete prior-checking case: ARACHNE, a system notified for prior-checking to the EDPS by the European Commission's DG Employment in May 2013 (one of our session speakers today might recognise "his" case).

The purpose of the ARACHNE system is fraud detection; it is part of the Commission's fraud prevention and detection strategy in the area of Structural Funds. ARACHNE builds on the existing Commission Early Warning System, complementing it with publicly available information. It aims at identifying the most risky projects and thus helping auditors identify future targets for audit.

After analysis, the EDPS issued his opinion in February 2014 - like all our opinions, it is publically available on our website. I would like to share the three main recommendations by the EDPS, as they are more or less **representative for recommendations on anti-fraud measures of all EU institutions**:

Firstly, the requirement of a **specific legal basis**: As typical anti-fraud measure, ARACHNE aims to identify "bad clients". To do that, the database includes references to offences and criminal convictions. Processing such special categories of data comes under Article 10(5) of Reg. 45/2001. Given the sensitivity of such data, this requires safeguards. Consequently, processing may be carried out only if explicitly authorised by the Treaty or another legal instrument - or, if necessary, by the EDPS, subject to appropriate specific safeguards. The existence of a specific legal basis is key to safeguarding not only individual data subject rights and "fair process", but the legitimacy and transparency of the process as a whole and vis-à-vis the general public.

Secondly, a **high level of data quality** is required. It is the controller's responsibility under Article 4 of Reg. 45/2001 to ensure the quality of the data processed. That includes an obligation to make sure it is accurate and, where necessary, kept up to date. This applies in particular to the ARACHNE system, which complements the Commission database with publicly available information stemming from media. Again: getting anti-fraud right on the basis of sound facts obviously matters to the data subject. Think for example of the reputational and economic risks in the context of structural funds as in ARACHNE. But a solid facts-base is equally important for the legitimacy of anti-fraud action, be it preventive or repressive. Data quality is paramount in ensuring this.

Let me thirdly refer to the need to **inform data subjects** concerned about the controller, the purpose of processing, the existence of the right of access, the possibility to submit a complaint to the EDPS and so forth. Articles 11 and 12 of Regulation 45/2001 contain a shopping list of what EU institutions need to tell data subjects about when they collect their data. This is a key transparency requirement vis-à-vis the general public. And, to the individual, it is key to exercising further data subject rights, such as access to their personal data or their rectification.

Whilst the follow-up of the particular case of ARACHNE is still in the making, other cases have drawn attention to two more issues I would like to address: the right of data subjects to access their personal data and the transfer of personal data.

Regarding the **data subjects' right to access their personal data**, we have very much advocated for balancing all interests involved in such requests.

When OLAF consulted us on the level of detail required in answering such a request, we argued that the possibility for the data subject to evaluate the accuracy of data and the lawfulness of processing needs to be balanced with the burden of the task for the controller. The potential risk for the fundamental rights and freedoms of the data

subject are significant where the data subject is the "person concerned" in an investigation, because of the obligation to ensure respect of the right of defence.

- In several prior-checks, the EDPS has established that in certain cases it may be necessary to *not* give direct access to the data subject at all. On the basis of exceptions foreseen by Article 20 of Regulation 45/2001, access can for example be deferred for as long as it would harm the proper functioning of an inquiry.

- Also, based on a consultation from the European Ombudsman, we have taken the position that the identity of whistle-blowers or informants should in principle not be disclosed. Exceptionally, disclosure to judicial authorities should be considered where required under national judicial procedures and/or in case of malicious false statements.

Those few examples illustrate that correct applying rules and principles of data protection whilst ensuring transparency of the EU administration is a balancing act.

The same is true for **transfers of personal data**, which for anti-fraud measures often involve transfers outside the EU administration, including to international organisations. The transfer of personal data to *other EU institutions or bodies* is covered by Regulation 45/2001 and, in the case of OLAF, the OLAF Regulation. It is crucial that such transfers only take place to the extent *necessary* at any particular stage of a procedure. If personal data are transferred to judicial authorities in the *Member States* or to Europol or Eurojust, or where OLAF receives information from authorities in the Member States, additional rules become relevant as well.

International flows of personal data to third countries and/or international organisations deserve specific attention, as the receiving jurisdiction may often not have data protection rules that offer protection similar to that provided in the EU. For this reason, Regulation 45/2001 contains additional rules for such transfers, just like the data protection legislation in the EU Member States.

The EDPS has advised OLAF in different circumstances in this field. While such transfers may be very useful for investigations, they need to be framed by clear rules to avoid undue impact on the rights and freedoms of individuals. So on our advice OLAF has developed Data Protection Clauses. These clauses are part of the administrative cooperation arrangement that OLAF agrees with international partners.

Summing up, these examples have shown that the aim of the EDPS' work as a supervisory authority is not to make life difficult for investigators, but to make sure that the processing of personal data for anti-fraud purposes by OLAF and others happens in full compliance with the law. Think of us as a critical friend if you will - we understand what they do and also how and why, but are not afraid to say "stop" if things should go wrong.

***

So, after explaining how we supervise OLAF and sharing some specific cases with you, what are the main takeaways from our supervision of OLAF? Which lessons learned are also relevant in a wider perspective? Let me mention two points at this stage:

- Firstly, in the case of OLAF investigations, Regulation 45/2001 is *applied in the field of investigatory activities*. Relevant exceptions are used, not as a general rule, but when necessary and allowed by the Regulation. This shows that a comprehensive protection scheme involving all areas of EU policy is a feasible solution. This does not exclude sufficient attention for the specificities of investigation activities, including those by law enforcement agencies!

- Secondly, the **Data Protection Officer** at OLAF has been playing a key role in developing internal compliance. This positive experience and others explain why the EDPS promotes the idea of introducing a Data Protection Officer as front-line data protection specialist beyond the EU administration in the context of the GDPR.

So much for the general "lessons learned" from anti-fraud measures by EU administrations. The EDPS will of course continue to be an active partner in providing all EU institutions with practical and dynamic solutions in applying anti-fraud schemes that respect data protection principles.

The EDPS has already issued general **guidelines** on the international transfer of personal data to third countries as well as the rights of data subjects, including their right to access their data.

These guidelines offer practical guidance and best-practice examples in reconciling the public interest for transparency and the individual's rights to privacy and data protection generally.

As regards specific anti-fraud activities by EU administration, the EDPS has issued guidelines on managing conflicts of interest and on conducting administrative inquiries and disciplinary proceedings. At the EDPS, we believe that data protection principles may considerably strengthen the management and prevention of conflicts of interest and they are a precondition for ensuring "fair process".

Let me note that EU bodies must be fully accountable for how they process personal information, because to demonstrate exemplary leadership we must be beyond reproach. EU institutions and bodies should lead the way in demonstrating accountability in practice.

***

"Lessons learned" and "accountability" are also two of the key words for the EDPS' contribution to the GDPR

We are now about a month away from the anticipated agreement by the Council on a common position for reform of the EU's data protection framework, a move which will immediately trigger the trilogue negotiations with the European Parliament and Commission – the home straight of a marathon process.

At the same time, we are in the middle of a number of tracks for determining rules and standards for personal data flows between the EU and other countries, notably the US - the Safe Harbor agreement by no means the only example.

We need a new deal on data protection in the EU and we need it fast. The new data protection regulation is just the beginning: we need to mainstream the rights of the individual throughout all policies, whether on law and order, financial services regulation, exchange of health data, or competition and consumer law.

The Revision of Regulation 45/2001 gives us an opportunity for future oriented rules for the EU institutions.

On each of these fronts the EDPS will engage proactively and honestly. And we will broaden the debate beyond politicians, privacy lawyers and regulators.
There is still a lot to play for in the EU data protection reform.

- Definitions
- Scope
- Individual rights eg RTBF and data portability
- Purpose limitation
- The 'one-stop shop'
- Data transfers
- Red tape and burdens
- Sanctions

But time is running out.

In a few weeks, the Council is likely to adopt a common position, and they will begin formal negotiations with the Parliament.

As advisor to the institutions, the EDPS will shortly afterwards publish a position paper, highlighting the main issues from a fundamental rights perspective, but moreover offering pragmatic suggestions for resolving the differences between the institutions:

Suggestions for making the rules simpler and easier to comply with.

Suggestions for ensuring that the rules will be relevant for a generation.

On the basis of our experience in implementing the data protection rules for EU institutions, as laid down in Regulation 45/2001, we will be proactive in our cooperation with the EU legislator to modernise them in parallel with the GDPR.

We intend to work with the European Parliament, Council and Commission to ensure current rules set out in Regulation 45/2001 are brought into line with the General Data Protection Regulation and a revised framework enters into force by the beginning of 2018 at the latest.

Thank you for listening. I look forward to our discussion.