International Ombudsman Institute
Institut International de l'Ombudsman
Instituto Internacional del Ombudsman

the federal Ombudsman
20 years

# IOI-EUROPE CONFERENCE
## THE OMBUDSMAN IN AN OPEN AND PARTICIPATORY SOCIETY

Brussels I Senate
1-2-3 I 10 I 2018

## Emily O'Reilly, European Ombudsman

## The Ombudsman in his/her relations to access to information and to transparency

Thank you for asking me to participate in this session, which addresses a theme which is central to the successful operation of an Ombudsman's office and the work we do, day in, day out. An investigation is independent, fair, and carried out in full command of all of the facts only if we have access to all information that we consider relevant.

The issues which are raised here are ones which, I'm pleased to say, do not cause difficulty for me or my staff very often. When they do arise they can be challenging and can have far-reaching consequences, but that is partly because problems in this area are, for us, exceptional.

I'll shortly talk about two of those situations, quite different in type, that did cause me problems but first, some context in terms of the constitutional framework.

Within the institutions of the European Union, the key principle which governs the working arrangements is found in Article 4 of the Treaty of the European Union, namely the duty of sincere cooperation.

This applies to the Union and to its Member States and requires us all to assist each other in carrying out our respective tasks, which flow from the Treaties, in a spirit of full mutual respect. Strictly speaking this obligation does not apply to relations between the European Ombudsman and those who are subject to the Ombudsman's mandate, but in practice we do cooperate with each other and respect each other's roles and place within the EU constitutional framework.

My task is to investigate complaints from citizens into instances of maladministration in the EU institutions and other bodies. I am elected by the European Parliament and my independence is enshrined in the Treaties. The Parliament has set out the legal framework for performing my tasks in my governing statute. This includes an obligation on EU institutions to supply my office with any information I have requested from them and to give

me access to the relevant files. Clearly, as an Ombudsman, I have to be able to access the administrative files I am mandated to review.

As you would expect, there are corresponding obligations not to disclose classified information or documents, but otherwise my powers of access to information are very wide. I can also require officials to testify formally in the course of an inquiry. That has rarely been necessary, but it is an important and powerful backstop.

In the vast majority of cases, the inspection of documents and access to the relevant files takes place without incident. We are now being given electronic access to most of the key documents we need, which obviates the need for case handlers to travel to wherever the files are held.

So, for example, in a current inquiry into a complaint where public access to documents was refused by Europol, the documents have been sent to my office electronically, but securely, under password protection. I welcome these developments and the trust in my office that this demonstrates. I only hope that the trust in the technology is equally well-founded!

But it was in another access to documents case involving Europol, that I faced an immovable obstacle to the fulfilment of my mandate. The inquiry concerned public access to a document held by Europol concerning its activities under the EU-US Terrorist Finance Tracking Program Agreement.



That agreement, concluded between the EU and the US in 2010, provides that the EU may transmit financial messaging data of EU citizens to the US Treasury Department in order to track terrorist activity. The data is held in Belgium by an organisation known by the acronym SWIFT. Europol's role is to validate requests from the US for the transmission of the data, although it did not actually have access to the data itself.

In June 2013, my office received a complaint from a member of the European Parliament, about Europol's handling of an access to documents request for public access to a report by Europol's Joint Supervisory Body, which oversees Europol's data protection compliance, on the implementation of the EU-US Agreement. In other words, a report that would indicate whether the data protection aspects of the agreement were working properly.

As is normal and necessary in an inquiry regarding access to documents, I asked my staff to inspect the document, so that we could assess the case for and against public disclosure. Europol cooperated with my inquiry team and we agreed strict security arrangements for the inspection.

However, what then transpired was that the Agreement between the EU and the US incorporated a secondary agreement on what were called "technical modalities" on implementation.

Under these "technical modalities", no information transmitted by the US Treasury Department, including information regarding types or categories of messages, could be shared with any other party without the express written authorisation of the US Treasury Department. Despite Europol's efforts to secure the relevant authorisation, it was refused by the US authorities on the grounds that the "need to know" requirement was not met.

So, by virtue of this US veto, I was effectively prevented from fulfilling the role that the democratically elected European Parliament had entrusted to me as Ombudsman, an office to which I had been duly elected by that Parliament. I personally met with the then US Ambassador to the EU and if I recall, some officials from the State Department, but they refused to accept the European Ombudsman had the right to see this record to ensure that the refusal was valid.

I therefore had no alternative but to close my inquiry without reaching a conclusion. However, I asked the European Parliament to consider whether it was acceptable that, as European Ombudsman, I should be prevented from doing my job, by an agreement with a foreign government, which, as a side agreement on technical aspects of implementation, had never been sent to the European Parliament or the Council of the European Union for approval. I pointed out that, in the absence of Ombudsman scrutiny, there was effectively no oversight of the Swift agreement as Europol, as I pointed out earlier, doesn't actually see the records that are sent from the EU to the US.



The most recent occasion on which my office faced some logistical issues over the inspection of relevant files, was in my inquiry into the European Commission's appointment of a new Secretary General earlier this year. For the purposes of that inquiry, I had written to the Commission, stating that I had decided that it was necessary to inspect *"all documents, whether in electronic or paper format, including correspondence, notes, memos, emails, and all legal advice, from 1 September 2017 until 18 April 2018, relating to the appointment of the new Secretary-General*".

However, at the first inspection meeting my inquiry team were shown just two folders of documents and one separate additional document. Many of these were marked "confidential" and we were unable to take copies. My inquiry team had to clarify the broad scope of the inspection requirements, even though this had been perfectly clear in the initial inspection request.

Consequently, 2 weeks after the first inspection, a further 10 days of inspection meetings took place over a 3-week period. No further copies of documents were permitted. My inquiry team were required to put any electronic devices into a secure container in the room, so they could not be used. The room itself had no natural light and a security guard was present at all times as my team took notes from thousands of records, by hand.

In my view, those conditions can be described only as oppressive. This was not an inquiry into a matter of national security or serious criminal activity but rather an inquiry into the adminsitration of a recruitment process.

I do need to emphasise that the two examples I have set out in some detail today were exceptional in my experience as European Ombudsman and I hope they remain so. My office enjoys good cooperation with the institutions and other bodies and agencies of the EU and the increasing acceptance of electronic communication of even sensitive files as the norm, is very welcome.

I also understand the need for organisations such as ours, which demand high administrative standards of others, must themselves adopt and demonstrate such high standards. It would undermine the trust of citizens and the authority of our offices and decisions if we did not ourselves reflect good practice. So whilst impact, relevance and visibility continue to be the cornerstones of my strategy, maintaining a high level of transparency of what we do and how we do it is essential. Ombudsmen must also show that they meet the high standards of ethical conduct, which are rightly required of independent public office holders.

Good communication tools, including a website that is informative and easy to navigate are a necessary part of public accountability. My office's website includes information about remuneration, mission expenses, gifts, hospitality and declarations of interest. We cannot do anything other than lead by example in relation those principles and values of public life which, on behalf of citizens, we require other public bodies to uphold and demonstrate.



Likewise with public access to documents and information about our services. We must adhere to the rules which others rightly expect us to promote and enforce on their behalf. I'm sure we all abide by the transparency laws that apply in our respective jurisdictions. It is vital that we do. Otherwise we do not deserve to enjoy the trust and respect of those we serve and whose legitimate interests we try to safeguard.

I look forward to hearing other colleagues' reflections on these issues, based on their experiences, and to the discussion which will follow.

Thank you.