Frontex and Data Protection

Another Rule of Law Challenge in Sight?

Sarah Tas

09.09.2022 doi: 10.17176/20220909-230639-0

Frontex has become notorious for its multiple fundamental rights violations, including pushbacks. The problem of fundamental rights infringements associated with the Agency has been lasting for years, leading ultimately to the resignation of the Executive Director. What I argue in this post is, first, that the fundamental right to the protection of personal data by Frontex has not yet received sufficient attention by scholars and EU institutions. Second, data protection within the Agency needs to be strengthened to prevent any future new scandals.

Frontex's growing intelligence role

Frontex's mission is to coordinate border management and support Member States in controlling the Schengen external borders. To do so, the Agency provides technical and operational assistance to the Member States by organising and coordinating joint operations, pilot projects, rapid border intervention teams, and return operations. On first sight, Frontex's core role is not data processing, instead, the Agency plays a distinct role on the field. However, when one takes a closer look, a segment of Frontex's actions also touches upon personal data. This intelligence role of Frontex continuously increases over the years, with regular legislative amendments.

When Frontex was first established in 2004, there was then little discussion regarding its intelligence task. Only two provisions of the original Frontex Regulation were deemed relevant. First, Article 11 on information exchange systems, and second, Article 13 on the cooperation with third countries, international organisations, and Europol, notably through working arrangements. However, the latter did not expressly grant the possibility of exchanging personal data. As an example, the Strategic Co-operation Agreement between Frontex and Europol, signed in 2008, initially excluded the exchange of personal data. While in theory no provision included the processing and exchange of personal data, in practice Frontex was still processing such data, in the context of joint return operations. The competence to process personal data was formally introduced in a 2011 amendment of the Frontex Regulation.

With the start of the 'migration crisis' in 2015, and increased cross-border criminality linked to terrorism, an additional shift appeared in the role of Frontex with personal data. Whilst several examples can illustrate this, two of them will be discussed within this contribution. First, the establishment of the European Border Surveillance System (EUROSUR) deserves further scrutiny. This is a mass surveillance and data exchange programme, that allows connecting National Coordination Centres in the Member States with each other and with Frontex. Second, enhanced cooperation occurs in the field, for example in the hotspots (European Agenda on Migration 2015). Frontex cooperates with other EU agencies to support the Member States facing high migratory pressure, through the identification, registration, return, and criminal investigations. Frontex may collect personal data during the screening and identification phase, that may be exchanged with other actors. The European Border and Coast Guard (hereafter EBCG) Regulation adopted in 2016, put Frontex's formal mandate in line with its intelligence role that was starting to unfold in practice. Section 2 of the 2016 Regulation solely focused on 'information exchange and data protection', and mentioned the information exchange systems, as well as the collection and purposes of the processing of personal data. Furthermore, Frontex can since then process personal data in the context of its activities, including joint

operations, pilot projects, rapid border interventions, return interventions and risk analyses. Article 52 also emphasized the cooperation with third countries, international organisations, and various EU bodies, including the exchange of personal data. Thus, a real jump to a more intelligence task for Frontex is to be witnessed then, which is further emphasized by the inclusion of EUROSUR in the Regulation with its 2019 amendment. Regulation (EU) 2019/1896 added a reference to the European Travel Information and Authorisation System (ETIAS) (which will be analysed by Amanda Musco Eklund in Part 1 of her blogpost). Frontex will be responsible for setting up and running the Central Unit of the system, giving the Agency thereby a key information role. The system is not yet active but is planned to become operational and mandatory in 2023.

In summary, while initially Frontex has not been entrusted with information task and data processing and exchange, these essential functions of the agency cannot be overlooked. This subsidiary role of Frontex can have a severe impact on the individuals' rights and freedoms, and it must be accompanied by strong safeguards and notably robust supervision.

Frontex's compliance with data protection: a necessity to step up supervision

Having reviewed Frontex's growing intelligence role, this section further explores the links between data protection and the work of the Agency. In this regard, Council Regulation (EC) No 2007/2004 establishing Frontex, mentioned in Recital 19 that Frontex must apply Regulation (EC) No 45/2001 on the protection of personal data by Community institutions and bodies. No other provision mentioned data protection or supervision at the time. While Frontex was already processing personal data, no measures were taken to implement data protection rules. With the 2011 amendment of the Frontex Regulation and the formal introduction of the Agency's processing of personal data, came also provisions of data protection and supervision. Recital 25 formally introduced the European Data Protection Supervisor (EDPS) as the monitor the processing of personal data by the Agency. However, the EDPS already performed its supervisory role prior to this change. The latter approach diverged from that of other third pillar agencies, like Europol and Eurojust, that were supervised at the time by the Joint Supervisory Body. Even if the EDPS started its work early on with Frontex, the use of its powers in practice has been limited.

From 2009 to 2014, the EDPS delivered several opinions resulting from prior checking procedures or consultations (for example Case 2009-0281 and Case 2010-0071) and comments, notably on the draft Frontex Regulation. While the EDPS did some supervisory work over Frontex, it essentially remained silent on it in the Annual Reports. In the Annual Report of 2013, Frontex was mentioned only three times, simply to give the name and e-mail address of the Data Protection Officer. Europol, however, was mentioned 19 times, even if the Joint Supervisory Body was still the official supervisor at that time. Additionally, the EDPS also carried out visits to the premises of Frontex, drafted reports notably on the use of personal data in risk analysis, and opinions on further legislative proposals. However, the supervisory action of the EDPS remained essentially limited, as the comparison with Europol shows.

In 2016, the EDPS became the official supervisor of Europol. A special team was set up, and within a year, the EDPS had already dealt with two complaints, three prior consultations, one inspection, and four inquiries – whilst they conducted one operational visit (see Annual Report 2017). The same treatment was not reserved for Frontex. In fact, in 2017, no publicly available opinions, and recommendations were made for Frontex. Since then, every EDPS Annual Report had a specific section of approximatively 5 pages, focusing on 'Supervising Europol'. This level of scrutiny has never been carried out for Frontex. The EDPS continued its supervisory work over Frontex with some prior check opinions, formal comments, and decisions. However, these could be counted on the fingers of one hand. It would be in bad faith to say that the EDPS does not supervise Frontex. However, the supervision remains quite limited. It is undeniable that more supervision is needed, given the widespread powers of

the Agency in this field. Finally, until today the EDPS has never used its corrective powers *vis-à-vis* Frontex (for example, the power to impose a temporary or definitive ban on a processing operation, impose an administrative fine etc.).

Need for maturity in the data protection culture of the Agency

This blogpost shows that Frontex is playing an increasingly important role in the processing and exchange of personal data in the Area of Freedom Security and Justice. The blurring of boundaries between law enforcement and migration purposes further enhanced this information-related role of Frontex. As this role is a *de jure* and *de facto* reality, appropriate data protection provisions and supervision are of key importance.

Data protection provisions were introduced in the 2011 amendment of Frontex Regulation, with clarifications on the processing of personal data in joint return operations (Article 11b), during joint border surveillance operations, pilot projects and rapid interventions (Article 11c), and on security rules for classified information and non-classified sensitive information (Article 11d). However, the Regulation failed to contain specific rules on the data subject's rights, and the obligation of the data controller *vis-à-vis* data subjects. Additional data protection provisions came with the 2016 EBCG Regulation, and with its most recent 2019 amendment. Provisions on purpose limitation and data protection were strengthened, and rules on data retention were added. However, what is problematic, is that exemption to data protection provisions were further enhanced, giving thereby the possibility to more extensively circumvent EU's data protection rules (see Articles 51 and 82 of the 2019 Regulation).

A data protection culture within Frontex started to emerge only 10 years ago, in 2011. This can be contrasted with Europol for example, where data has been at the core of its function since its establishment: data protection was present in the Europol Convention (1991). It included notable provisions on the standards of data protection and responsibility in data protection matters. The delay in the data protection culture and awareness within Frontex, particularly by the staff, and the limited supervision around it make it an agency that still has a lot to learn. While it is not surprising that Europol gets more attention from the EDPS, given the amount of data Europol processes, it is also particularly important for the EDPS staff to familiarize themselves further with Frontex, and to enhance its supervision to prevent violations of data protection by the Agency.

This blogpost demonstrated a shift in Frontex's role, with the Agency gaining a larger intelligence task. This increasingly relevant role of the Agency with respect to data management has been followed by the addition of data protection provisions in the Agency's Regulation and supervision by the EDPS. However, more efforts are needed to ensure an efficient data protection culture and supervision within the Agency. This seems to have been acknowledged by the EDPS, which changed its approach and set up a team supervising 'the Area of Freedom, Security and Justice'. This is an excellent first step, not only to supervise the work Frontex and other EU agencies in this area, but also the increasing data exchanges between them.

ABOUT THE AUTHOR

Sarah Tas
Sarah Tas is an Assistant Professor of European and Comparative Administrative Law at Maastricht University.

SUGGESTED CITATION

Tas, Sarah: Frontex and Data Protection: Another Rule of Law Challenge in Sight?, Verfassungsblog, 09.09.2022, doi: 10.17176/20220909-230639-0.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20220909-230639-0.