ONTIER

26th September 2017
#16

Index

INDEPENDENT SUPERVISORY AUTHORITIES

Every Member State has to appoint one independent public authority for a minimum period of four years, who will be in charge of overseeing and enforcing the application of the Regulation and cooperating with the other State Members' authorities in their investigation into certain businesses and organisations.

Current situation

Directive 95/46/EC establishes the duty to designate a public authority to oversee and enforce the proper application of the Directive (as transposed into national law). These supervisory authorities must be absolutely independent and have at least a group of competences *a posteriori*, such as to publish periodic reports or to refer matters to the judicial authorities.

Supervisory authorities can only exercise their functions within the territory of their respective Member State, but it is possible for them to exercise their authority at the request of an authority of another Member State.

As developed by Article 28 of Directive 95/46/EC, supervisory authorities have generally three groups of powers: investigative, intervention and procedural powers. In addition, supervisory authorities must hear all claims brought by any person concerning the protection of his/her rights and, afterwards, inform the person about the outcome.

All decisions of supervisory authorities are subject to appeals and they are required to present (public) reports on their activities at regular intervals, co-operate with other supervisory authorities when necessary and be subject to professional secrecy.

On the other hand, Data Controllers and Data Processors or their representatives must notify supervisory authorities before any processing operation and, afterwards, register them. Some operations may be also subject to prior checks by the relevant supervisory authority/ies.

What's new?

The main characteristics and functions of independent supervisory authorities under the GDPR are essentially similar to those provided for by the Directive.

However, the GDPR regulates both new and existing issues in a more detailed way. In addition to their duty of monitoring the application of data protection law, supervisory authorities now have the obligation to protect the fundamental rights and freedoms of natural persons in relation to the processing of their data.

With regards to their financing, unlike the Directive 95/46/EC where supervisory authorities were not granted a special budget, the GDPR states at Recital 120 and Article 52 that Member States now have the obligation to grant a separate budget for their supervisory authorities.

Member States can now also establish more than one supervisory authority within their territory and they are free to set and regulate their establishment and any required qualifications.

The requirement for independence of the supervisory authorities, which was also present in the Directive, is now more specifically regulated by Article 52(2) of the GDPR, which establishes that they cannot be subject to direct nor indirect influence and Article 52(6) that specifies the need for a functional independence from their government.

The '*one stop shop'* principle established by the GDPR (Article 56) is, as seen, another major novelty: now when the case of a cross border processing occurs, the lead supervisory authority will be the one of the Member State where the company's main establishment is based (the lead supervisory). However, there is the possibility for the lead authority to refuse to cede the control, case in which it must coordinate with the other concerned authority. Please see article 15 for more details on this.

The GDPR lists different tasks and powers of supervisory authorities to assist them with their role. The most relevant tasks include:

a) Advising on legislative and administrative measures;

b) Monitoring relevant developments (particularly those of information and communication technologies and commercial practices);

c) Adopt standard contractual clauses;

d) Periodically review the issued certifications of controllers and processors;

e) Authorize contractual clauses related to cross border arrangements and provisions in administrative arrangements that include data subject rights;

f) Charge a reasonable fee based on administrative costs or to simply refuse to act on requests for information, advice, authorization, intervention, consultation, and others when such requests are unfounded or excessive; and

g) Publish a list of certain processing operations which may require a data protection impact assessment and, when this assessments show that the processing would carry a high risk, give advice prior to the processing.

Regarding their powers, supervisory authorities can:

a) Request any information;

b) Audit companies;

c) Access all necessary data and information;

d) Access any premises of the controller and/or processor;

e) Issue warnings, reprimands, fines (up to € 20 million or 4% of annual worldwide turnover of the preceding year, whichever is higher) and bans (both temporary and permanent) in case of breach of the Regulation;

f) Withdraw certifications;

g) Order the suspension of cross border data flows;

h) Issue certifications and approve their criteria;

i) Adopt or authorize certain standard contractual clauses;

j) Authorize administrative arrangements in cross border processing; and

k) Approve binding corporate rules.

The GDPR also establishes obligations on Data Controllers and Data Processors in dealing with their supervisory authority; for instance, they are required to notify the authority about any breach of personal data within 72 hours after they become aware of it (Article 33) and to communicate the contact details of any data protection officer so designated (Article 37.7).

Furthermore, supervisory authorities may have wider or more attributions, as Article 58.6 of the GDPR allows each Member State to provide them with additional powers.

Aside from the power and attributions of supervisory authorities, the GDPR also regulates other important aspects such as their responsibility over the decisions they make. Article 78 of the GDPR states that any natural or legal person affected by a decision will have the right to bring a proceeding against the relevant supervisory authority before the courts of its Member State and, when fair, will have the right to an effective judicial remedy.

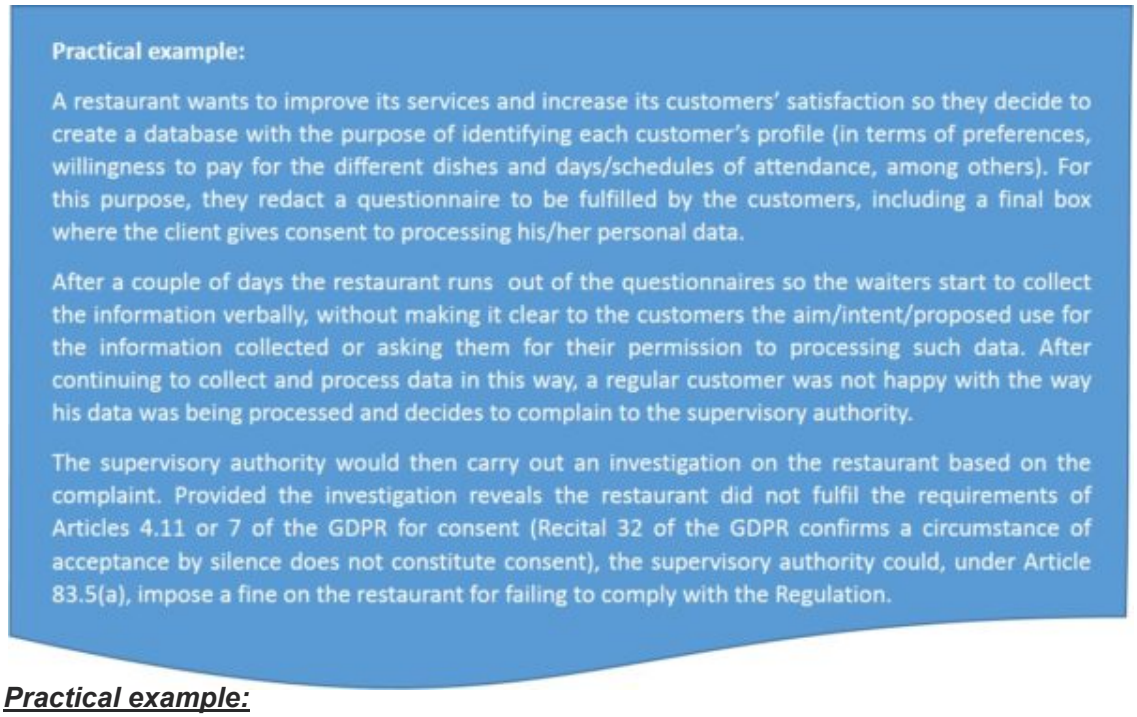
When it comes to the expiry of the term of duties, resignation or dismissals of supervisory authorities, the Regulation sets this out in a clear manner. Article 53(3) and (4) of the GDPR states that the duties of a supervisory authority ends in the event of expiry of the term in office, resignation or compulsory retirement and dismissals can only proceed when there is a serious misconduct or it does not fulfil the conditions.

Finally, all of the 28 different independent supervisory authorities of the Member States will constitute the European Data Protection Board, an independent body with legal personality charged with the responsibility of ensuring consistency in the application of the GDPR. When more than one supervisory authority exist in a Member State, a representative will have to be appointed as the principal contact for the other authorities, the Board and the Commissions. The Board plays an important role as national supervisory authorities are required to co-ordinate, report and proceed in accordance with its opinions, guidelines and monitoring to ensure consistent application of the Regulation across the EU.

What to do to adapt?

Both Data Controllers and Data Processors must actively cooperate with their competent supervisory authority. Among other duties, they must notify the supervisory authority about any breach of personal data within 72 hours of becoming aware of it; they must consult with the supervisory authority in respect of any of their protection impact assessment which indicates that a certain processing might carry a risk; they have to notify the supervisory authority the contact details of any data protection officer they so designate; and, if asked, they must present their processing activities record.

All the above should also be taken into account by non-EU companies who offer their services or goods or monitor people’s behaviour within the EU territory, given the broader territorial scope of the GDPR.



Practical example:

A restaurant wants to improve its services and increase its customers' satisfaction so they decide to create a database with the purpose of identifying each customer's profile (in terms of preferences, willingness to pay for the different dishes and days/schedules of attendance, among others). For this purpose, they redact a questionnaire to be fulfilled by the customers, including a final box where the client gives consent to processing his/her personal data.

After a couple of days the restaurant runs out of the questionnaires so the waiters start to collect the information verbally, without making it clear to the customers the aim/intent/proposed use for the information collected or asking them for their permission to processing such data. After continuing to collect and process data in this way, a regular customer was not happy with the way his data was being processed and decides to complain to the supervisory authority.

The supervisory authority would then carry out an investigation on the restaurant based on the complaint. Provided the investigation reveals the restaurant did not fulfil the requirements of Articles 4.11 or 7 of the GDPR for consent (Recital 32 of the GDPR confirms a circumstance of acceptance by silence does not constitute consent), the supervisory authority could, under Article 83.5(a), impose a fine on the restaurant for failing to comply with the Regulation.

TEAM

Joaquin Muñoz Rodríguez (Spain)
Pablo Uslé Presmanes (Spain)

Derek Stinson (UK)
Paula Enríquez (UK)

Ana Rocha (Portugal)
Joana Cunha de Miranda (Portugal)

Luca Pardo (Italy)
Giulio Ciompi (Italy)

Read more:

about us

Share on:

Linkedin Twitter

Subscribe:

our Newsletters

Contact us:

Website | LinkedIn

Rua Vitor Cordon Nº 10A - 1249 - 202 Lisboa | Portugal
Tel. (+351) 213 223 590 / Fax (+351) 213 223 599

Rua Pedro Homem de Melo, n.º 55, 8º piso - 4150 - 599 Porto | Portugal
Tel. (+351) 223 190 888 / Fax (+351) 220 924 945

PORTUGAL / **SPAIN** / **U.K** / BOLIVIA / / BRAZIL / CHILE / CHINA / COLOMBIA USA / ITALY / MEXICO / PERU / VENEZUELA

This article is provided for information purposes only and does not constitute legal advice. Professional legal advice should be obtained before taking or refraining from any action as a result of the contents of this document. If you have any queries regarding this article, please contact CCA Ontier or ar@cca-ontier.com.