PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 7:

Independent Supervisory Authority

Independent Supervisory Authority

While international data protection agreements remain largely non-prescriptive on enforcement, in order to give effect to the fundamental right of data protection and its principles, legislation must provide for the establishment of an independent supervisory authority. A supervisory authority requires this statutory footing in order to establish clearly its mandate, powers and independence.

Models and Structures

Two models of enforcement have been considered: the creation of an independent supervisory authority, and a ministry-based model.

Of the seven international agreements and standards relevant to data privacy, five require the establishment of an independent supervisory authority. While the OCED Principles did not call for an independent supervisory authority, the EU model, both the GDPR (previously Directive 1995) and the Convention 108 of the Council of Europe, did - 90% of countries with data protection laws have opted for this model. Having an independent supervisory authority is also directly relevant to an assessment of adequacy as it is essential for oversight and enforcement.

However, it is important to note that in many jurisdictions, such as Mexico and the UK, a single institution has been set up to serve both as a regulator and enforcer of laws pertaining to access to information and data protection. This combination of functions should not contradict the mandate, functions and powers of the enforcement authority, or independence from the Executive.

Furthermore, some countries have opted to have multiple independent supervisory authorities. In Germany the regulation of data protection in relation to public and private bodies happens at the state level, and then there is a Federal Data Protection Commissioner which monitors federal authorities and other public bodies under federal government control.

Structure, Mandate and Powers

The mere establishment of this independent authority is not sufficient. The law must ensure the following:

Structure

- Process for establishment and appointment: The law should provide for a process and timeframe for the establishment of the authority and appointment of its head/ members.
- Composition and structure: The law should lay out the composition of this authority, including the skills and expertise required.
- Resources: The law must stipulate that the authority will be given sufficient resources, both financial, technical and human.
- Independent status: The law must stipulate that the independent data protection authority remains independent, in order to effectively and adequately fulfil its mission of enforcing the data protection framework.
  The authority should be free from external influence, and refrain from actions incompatible with the duties of the authority.
- Monitor and enforce: The authority must be given the task to monitor and enforce the application of the law. This would also require periodic review of activities of those who are subject to the law.

Mandate

- Mandate to investigate: The authority must be given the mandate to conduct investigations and act on complaints, by issuing binding orders and imposing penalties when it discovers that an institution or other body has broken the law. This includes being able to: demand information from the controller or processor, conduct audits, obtain access to all the information they may need for the purpose of the investigation, including physical access to premises or equipment used for processing, if necessary.
- Mandate to receive and respond to complaints: Both individuals and public interest/privacy associations should be given the right to lodge complaints with this independent authority. The independent authority should also be able to receive complaints of competent organisations based on evidence revealing bad practice before a breach has occurred.

- Mandate to provide advice: The authority should advise the relevant government bodies (depending on political system), as well as other public bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regards to the processing of their personal data.
- Provider of information: The work of the authority should include the provision of information to data subjects with regards to the exercise of their rights under the law in their country or elsewhere; the latter may require liaising with foreign supervisory authorities.
- Mandate to promote public awareness: Part of the role of the authority is to promote public awareness and understanding of data subjects' rights, risks, rules, and safeguards. This includes awareness of the recourses available to them for demanding and enjoying those rights, and the risks to be conscious of when it comes to the protection of personal data.

Power

- Power to impose sanctions: The independent authority must have the power to impose appropriate penalties, including fines, enforcement notices, undertakings, and prosecution. This process of sanction should not depend on submission of the complaint by a data subject but can be imposed pro-actively by the independent data protection authority.
- Issuing recommendations and guidelines: Derived from its power to investigate and impose sanctions, the independent data authority should also be capable of issuing recommendations and guidelines, outlining its interpretation of some provisions or aspects of a data protection law, either in general or directed to a specific sector. Given the fast pace of technological development, this is also a way to avoid data protection laws becoming outdated and obsolete.
- Special regulatory powers: Additionally, in some cases a data protection law can give the data authority powers to regulate certain aspects of the law, for example to update definitions, security requirements, and approve trans-border data flows.

Taking action when the law is broken

The types of sanctions/ penalties which could be imposed vary, but may include:

- Administrative Fines, For example, under the GDPR, fines are set at €20, million or 4% of annual turnover; in South Korea, it is 3% of annual turnover.[1]
- Criminal offences (individual responsibility) for certain actions, for example knowingly or recklessly, without the consent of the data controller, obtaining or disclosing personal data.
- Direct liability for directors of companies

References

1 2014-2017 Update to Graham Greenleaf's Asia Data Privacy Laws: Trade and Human Rights Perspectives, University of New South Wales Law Research Series, 2017