Administrative fines

At a glance

- Supervisory authorities are empowered to impose significant administrative fines on both data controllers and data processors.
- Fines may be imposed instead of, or in addition to, measures that may be ordered by supervisory authorities. They may be imposed for a wide range of contraventions, including purely procedural infringements.
- Administrative fines are discretionary rather than mandatory; they must be imposed on a case by case basis and must be *"effective, proportionate and dissuasive"*.
- There are two tiers of administrative fines:
  - Some contraventions will be subject to administrative fines of up to €10,000,000 or, in the case of undertakings, 2% of global turnover, whichever is the higher.
  - Others will be subject to administrative fines of up to €20,000,000 or, in the case of undertakings, 4% of global turnover, whichever is the higher.
- Member States may determine whether, and to what extent public authorities should be subject to administrative fines.

To do list

- ☐ Run a GDPR compliance gap analysis to identify areas of most material non-compliance and to prioritise mitigating steps, especially in relation to high risk processing activities.
- ☐ Update risk registers.
- ☐ Assess liability exposure under existing customer, supplier and/or partner arrangements, including by assessing contract liability limitation and exclusion clauses.
- ☐ Review insurance arrangements.

Degree of change

General considerations

Administrative fines are not applicable automatically and are to be imposed on a case by case basis. Recital 148 clarifies that in the case of a minor infringement, or where a fine would impose a disproportionate burden on a natural person, a reprimand may be issued instead of a fine.

There is currently a high degree of variation across Member States in relation to the imposition of financial penalties by supervisory authorities. Although arrangements under the GDPR make provision for maximum penalties and allow supervisory authorities a degree of discretion in relation to their imposition, Recital 150 indicates that the consistency mechanism may be used to promote a consistent application of administrative fines.

Each Member States may however lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

Maximum administrative fines

The GDPR sets out two sets of maximum thresholds for administrative fines that may be imposed for relevant infringements.

In each case, the maximum fine is expressed in € or, in the case of undertakings, as a percentage of total worldwide annual turnover of the preceding year, whichever is higher. Recital 150 confirms that in this context *"an undertaking"* should be understood as defined in Articles 101 and 102 of the Treaty on the Functioning of the European Union ("TFEU") (i.e. broadly speaking, as entities engaged in economic activity).

Infringement of the following GDPR provisions are subject to administrative fines up to €20,000,000 or in the case of undertakings, up to 4% of global turnover, whichever is higher:

- the basic principles for processing, including conditions for consent (Articles 5, 6, 7 and 9);
- data subjects' rights (Articles 12-22);
- international transfers (Articles 44-49);
- obligations under Member State laws adopted under Chapter IX; and
- non-compliance with an order imposed by supervisory authorities (as referred to in Article 58(2)) or a failure to comply with a supervisory authority's investigation under Article 58(1).

Other infringements are subject to administrative fines up to €10,000,000 or, in the case of undertakings, up to 2% of global turnover, whichever is higher. Contraventions subject to these maximum fines include infringement of the following obligations:

- to obtain consent to the processing of data relating to children (Article 8);
- to implement technical and organisational measures to ensure data protection by design and default (Article 25);
- on joint controllers to agree to their respective compliance obligations (Article 26);
- on controllers and processors not established in the EU to designate representatives (Article 27);
- on controllers in relation to the engagement of processors (Article 28);
- on processors to subcontract only with the prior consent of the controller and to process data only on the controller's instruction (Articles 28-29);
- to maintain written records (Article 30);
- on controllers and processors to co-operate with supervisory authorities (Article 31);
- to implement technical and organisational measures (Article 32);
- to report breaches when required by the GDPR to do so (Articles 33-34);
- in relation to the conduct of privacy impact assessment (Articles 35-36);
- in relation to the appointment of Data Protection Officers (Articles 37-39);
- imposed on certification bodies (Article 42-43); and
- imposed on monitoring bodies to take action for infringement of codes of conduct (Article 41).

In cases where the same or linked processing involves violation of several provisions of the GDPR, fines may not exceed the amount specified for the most serious infringement.

Factors to be taken into account

GDPR Article 83(2) lists factors to be taken into account when determining whether to impose an administrative fine and deciding on the amount of any fine to be imposed. These include:

- the nature, gravity and duration of the infringement having regard to the nature, scope or purpose of the processing concerned as well as the number of data subjects and level of damage suffered by them;
- whether the infringement is intentional or negligent;
- actions taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor;
- any relevant previous infringements;
- the degree of co-operation with the supervisory authority;
- categories of personal data affected;
- whether the infringement was notified by the controller or processor to the supervisory authority;
- any previous history of enforcement;
- adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
- any other aggravating or mitigating factors applicable to the circumstances of the case (e.g. financial benefits gained, losses avoided, directly or indirectly, from the infringement).

Where fines are imposed on persons that are not an undertaking, the supervisory authority should also take account of a person's economic situation and the general level of income in the Member State.

Where can I find this?

Article 83 *Recitals 148-152*