Under the new rules the level of fines has gone up significantly.

A business processes the personal data of EU residents and offers them goods and services, irrespective of whether payment is required; or
Where the processing by a business relates to the monitoring of the behaviour of EU residents in so far as their behaviour takes place within the EU

What this is designed to do is to ensure that organisations with lower revenues can potentially be punished severely (i.e up to a maximum of €20 million), and that equally organisations with bigger revenues can also potentially be punished severely (up to 4% of their annual global turnover). Aggravating and mitigating factors will be applied in an approach that follows EU competition law enforcement

It is likely that the new powers will be well used. Since the fee for data protection registrations is abolished under the Regulation, fines will be the main source of income for data protection regulators. The model for fines under the Regulation again follows the current competition law regime, and according to the European Commission they have levied around €6.5 billion in penalties over the last 5 years using these similar powers

For example, a US online payments processor with all its offices in the US, that handles the data of EU citizens, can be investigated, fined and even prosecuted by an EU regulator. Determining whether an organisation based outside the EU is caught by the EU rules or not may well prove challenging.

The highest level of fine will apply to infringements involving non-compliance with orders imposed by a regulator. which is stated under the Regulation as being up to 20 000 000 EUR, or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher

Additionally, an organisation located outside the EU will also have to have a representative in the EU if it falls within the new rules, even if the business doesn't have an EU presence already

will heighten this challenge forcing trustees to adapt their procedures and guidelines accordingly

➜ GDPR breach notification

Article 33 Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d)describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5.The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34 Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.