MAYER | BROWN

25 APRIL 2024

UK GDPR AND THE PRICE OF NON-COMPLIANCE: ICO ISSUES NEW GUIDANCE ON CALCULATING FINES

AUTHORS:

MARK A. PRINSLEY, OLIVER YAROS, REECE RANDALL, ONDREJ HAJDA, ELLEN HEPWORTH, ALASDAIR MAHER, ANA HADNES BRUDER, LIVIA CREPALDI WOLF, ALEKSANDER LARSKI, TRAINEE SOLICITOR

The Information Commissioner's Office (the **"ICO"**) has clarified the methods it will use to calculate the fines it will issue for breaches of data privacy law in the UK by publishing its latest Data Protection Fining Guidance (the **"Guidance**") on 18 March 2024.

The ICO oversees compliance with the UK data protection law, including the Data Protection Act 2018 (the **"Act"**) and the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the **"UK GDPR"**) (together, the **"UK Data Protection Law"**). The Act empowers the ICO to issue penalty notices for breaches of the UK Data Protection Law, with the maximum amount being the higher of £17,500,000 or 4% of the concerned undertaking's total worldwide turnover.

The ICO must produce and publish guidance on penalty notices and the last Regulatory Action Policy document was published in November 2018 (the **"2018 Policy"**). This latest Guidance replaces the sections of the 2018 Policy related to penalty notices. The Guidance applies to all new investigations and any investigations which started before 18 March 2024 where the ICO has not yet issued a notice that it intends to impose a fine.

WHICH INFRINGEMENTS CAN RESULT IN A FINE?

The ICO's power to impose fines for breaches of the UK Data Protection Law stems from subsection 155(1) of the Act, which cross-refers to section 149 of the Act. Businesses can be fined for infringements related to:

1. the seven principles of processing introduced by the UK GDPR;
2. the rights of data subjects protected by Chapter III of the UK GDPR;
3. the Chapter IV obligations of controllers and processors;
4. the notification requirements in cases of data breaches;
5. the principles for data transfers outside the UK; and
6. the payment of a fee to the ICO by a data controller.

Monitoring bodies and certification providers can also be fined for failing to observe their obligations under the UK Data Protection Law; a failure to comply with an enforcement, information, or assessment notice issued by the ICO can also result in penalties.

WHAT IS THE STATUTORY MAXIMUM ?

The Act provides for two different levels of a maximum fine that the ICO can impose for breaches of the UK Data Protection Law. The standard maximum amount is £8,700,000, or 2% of the undertaking's total worldwide turnover; the higher maximum amount is £17,500,000, or 4% of the undertaking's total worldwide turnover. In both cases maximum is set at the higher of the two amounts.

The standard maximum amount applies for infringements related to:

1. a failure to comply with Chapter IV obligations imposed on controllers and processors, or the obligations placed on monitoring bodies and certification providers;

2. a failure to comply with Article 8 of the UK GDPR, related to processing of personal data of children under 13; and

3. a failure to comply with Article 11 of the UK GDPR, related to the inapplicability of data subject rights where they cannot be identified.

The higher maximum amount will apply to all other infringements.

CONCEPT OF AN "UNDERTAKING"

Neither the UK GDPR nor the Act define the term "undertaking". Instead, the concept of an undertaking is derived from EU competition law. Recital 150 of the UK GDPR states that an “undertaking”, in the context of UK Data Protection Law, should be understood to be an “undertaking” in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union (“**TFEU**”), which prohibits anti-competitive agreements between undertakings and abuses of dominant position by undertakings. The TFEU similarly does not define “undertaking”; instead, its meaning has been developed through the jurisprudence of the Court of Justice of the European Union (the “**CJEU**”). In the Guidance, the ICO acknowledges that while any new Article 101 and 102 decisions will no longer bind UK courts, the concept is sufficiently well established in UK law through the previous UK and retained EU caselaw.

In terms of CJEU jurisprudence, an undertaking means any entity engaged in an *economic activity*, regardless of its legal status and means of financing. In determining whether an undertaking is engaged in an “economic activity”, consideration is given to whether the undertaking offers goods or services on a market or, whether, in principle, the relevant activity could be carried out by a private undertaking to make a profit. Crucially, a single undertaking may comprise multiple legal entities – as long as they form a "single economic unit".

Whether two entities form a single economic unit depends on their ability to act autonomously. Where they cannot, due to another entity exercising "decisive influence" over them, they belong to the same undertaking.

The ICO states that it will consider all relevant factors about the economic, organisational and legal links tying the two entities together when deciding if they form a single undertaking. There is a presumption that in cases of complete (or near-complete) shareholding, decisive influence is exercised by the parent company. This presumption is rebuttable, but such rebuttal is rare in competition law cases.

Familiarity with this concept is important because the ICO uses the *undertaking's* global turnover to calculate

the starting point of fines and to determine the applicable statutory maximum. Additionally, the ICO can hold a parent company jointly and severally liable for the infringements of its subsidiaries.

This will be important, by way of example, for private equity firms who may form a single undertaking with their portfolio companies; and for participants in joint ventures – as both parents may exercise decisive influence over the joint venture, and potentially be held jointly and severally liable for any of its infringement of the UK Data Protection Law.

FINES FOR MULTIPLE INFRINGEMENTS

The Guidance clarifies how the ICO will determine the statutory maximum fine for multiple breaches of the UK Data Protection Law. Article 83(3) of the UK GDPR states that the fine imposed for breaches related to "the same or linked" processing operations cannot exceed the statutory maximum prescribed for the gravest infringement.

The ICO will assess the facts of each case to decide if the conduct is the same or sufficiently linked; in doing so it will consider:

- whether the processing activities aim to achieve the same purpose;
- whether they relate to the same, or a similar group, of data subjects; and
- whether the activities take place in close proximity in time.

In cases of linked processing operations, the ICO may still impose a separate fine for each infringement if their sum does not exceed the applicable statutory maximum.

Where the infringements are not caused by the same or linked processing, the ICO can impose multiple fines; and their sum can exceed the statutory maximum even where the ICO discovered the infringements during the same investigation or where it issues a single penalty notice.

FACTORS CONSIDERED BY THE ICO WHEN DETERMINING IF A FINE SHOULD BE IMPOSED

The Guidance sets out three factors which the ICO will consider when determining whether a fine should be imposed:

1. the seriousness of the infringement;
2. any relevant aggravating or mitigating factors; and
3. the effectiveness, proportionality, and dissuasive nature of enforcement.

1. THE SERIOUSNESS OF THE INFRINGEMENT

The seriousness of an infringement will be assessed by reference to (i) its nature, gravity, and duration; (ii) whether it was intentional or negligent; and (iii) the categories of personal data affected.

In appraising the nature, gravity, and duration of the infringement the ICO will have regard to:

- whether the infringement is subject to the standard or higher statutory maximum amount;
- the processing being motivated by profit; and whether the processing is central to the activity of the undertaking;
- whether the processing was high-risk (e.g., when it applied new or innovative technology or automated

decision-making);

- any power imbalance between the data subjects and the controller;
- involvement of personal data of children or vulnerable individuals;
- the territorial scope and scale of the processing, including the number of affected data subjects and any complaints; and
- the level of damage suffered by data subjects.

The ICO will find that an infringement was committed intentionally where there is evidence that the undertaking knew that the conduct was likely to breach the UK Data Protection Law, or wilfully ignored a risk that it would do so. Such evidence can include the processing being authorised by senior management; or the processing being carried out despite advice being received about the risks involved.

On the other hand, the Guidance states that infringement resulting from human error; a failure to comply with a policy or applicable code of conduct; a failure to check published material for personal data; or a failure to process technical updates in a timely manner will likely be categorised as negligent.

Finally, the ICO will take into account the categories of data affected by the infringement. Predictably, processing of special category data and criminal offences data points to a higher degree of seriousness. However, the ICO will also consider if the processing involved "particularly sensitive" data, the disclosure of which is likely to cause damage or distress to data subjects. The Guidance provides the following as an examples of such data:

- location data;
- private communications, especially when involving intimate details or confidential information;
- passport or driving license details; and
- financial data.

2. RELEVANT AGGRAVATING OR MITIGATING FACTORS

In considering the seriousness of an infringement, the ICO will have regard to any aggravating or mitigating factors which arose in connection with the breach. Please refer to the table below to see what factors will be considered, and when they are deemed to be mitigating or aggravating.

Factor	**Indications to treat the factor as mitigating**	**Indications to treat the factor as aggravating**
Action taken to mitigate harm to data subjects	• Effective and appropriate action; or • Action taken before the undertaking became aware of the ICO's investigation.	Cannot be considered as an aggravating factor.
Degree of	• Going above and beyond the	• Failing to implement the

Factor	Indications to treat the factor as mitigating	Indications to treat the factor as aggravating
responsibility of the controller or processor	obligations prescribed by the UK Data Protection Law.	appropriate technical and organisational measures given the undertaking's size, resources, and the nature of processing.
Relevant previous infringements	Cannot be considered as a mitigating factor.	• Recent previous infringements; • Previous infringements concerning a similar subject matter; • Previous infringements arising in a similar manner; • Repeated infringements demonstrating a generally lax attitude towards compliance.
Degree of cooperation with the ICO	• Cooperation allowed the enforcement to conclude significantly more quickly or effectively; or • Cooperation limited the harmful consequences for people's rights and freedoms.	• Persistent and repeated behaviour delaying regulatory action.
Manner in which the ICO became aware of the enforcement	• Self-reporting, if the undertaking was not under a duty to notify and the ICO was not already aware.	Unlikely to be considered an aggravating factor.
Previously ordered measures	Unlikely to be considered a mitigating factor.	• Failure to implement previously ordered measures with regard to the same subject-matter. • Note: A failure to implement a measure ordered in an enforcement or penalty notice can constitute separate infringement.
Adherence to approved codes of	• Effective action taken by a monitoring body may result in no fine	• Failure to follow provisions of a code directly relevant to the

Factor	Indications to treat the factor as mitigating	Indications to treat the factor as aggravating
conduct	being imposed by the ICO.	infringement.
Other factors	• Pro-active reporting of a security breach to other regulators and engagement with their regulatory processes, where such engagement is not already prescribed by law.	• Fines will seek to negate any benefit which the undertaking derived from the breach.

3. THE EFFECTIVENESS, PROPORTIONALITY, AND DISSUASIVE NATURE OF ENFORCEMENT

The ICO will first consider whether issuing a penalty notice would be effective and dissuasive; afterwards, it will consider if it would be proportionate to do so. A fine will be a proportionate enforcement measure where it does not exceed what is appropriate and necessary in the circumstances to meet the regulator's objectives. The ICO will consider the seriousness of the infringement, the level of harm suffered by data subjects, and the size and financial position of the infringing undertaking.

The Guidance notes that the ICO will consider the desirability of promoting economic growth, as prescribed by section 108 of the Deregulation Act 2015; although it notes that this duty would not legitimise non-compliance with the UK Data Protection Law, which may distort competition and harm the position of businesses investing in compliance procedures.

CALCULATION OF THE FINE

ASSESSING SERIOUSNESS

The ICO will determine the starting point of a fine by reference to the relevant statutory maximum. The ICO will categorise the infringement according to its degree of seriousness, with three categories available. For lower degree of seriousness, the fines will range from 0% to 10% of the applicable statutory maximum. For medium degree of seriousness, the range is 10% to 20%; with the higher degree of seriousness covering the range from 20% to 100%. The scale is irregular to reflect the varied conduct which can lead to an infringement.

The ICO did not provide further guidance on what factors it will consider to determine a specific number within these ranges; or how it will determine which category an infringement falls into. As the Guidance represents a departure from the 2018 Policy, future enforcement notices will be an important source of information. The ICO will also keep the ranges under review as it applies the Guidance in practice.

The table below sets out the monetary ranges to be referred to. In each case, the ICO will use the higher of the two amounts. This means that the turnover-based ranges will apply only to undertakings which generate more than £435 million turnover per year in cases of the standard maximum amount, and £437.5 million for the higher maximum amount.

Degree of seriousness	***Standard maximum amount***	***Higher maximum amount***

Lower degree of seriousness	Up to £870,000 or 0.2% of the global turnover.	Up to £1.75 million or 0.4% of the global turnover.
Medium degree of seriousness	From £870,000 to £1.74 million or from 0.2% to 0.4% of the global turnover.	From £1.75 million to £3.5 million or from 0.4% to 0.8% of the global turnover.
High degree of seriousness	From £1.74 million to £8.7 million or from 0.4% to 2% of the global turnover.	From £3.5 million to £17.5 million or from 0.8% to 4% of the global turnover.

ACCOUNTING FOR TURNOVER

The ICO recognises that the statutory maximum amounts apply to all undertakings, ranging from micro enterprises to multi-national corporations. To ensure that fines are effective, proportionate, and dissuasive, the fines imposed on small undertakings might be reduced in light of their turnover.

Turnover for these purposes means the amount derived from the provision of goods and services after the deduction of trade discounts and value added taxes. The turnover calculation will usually be based on the undertaking's last audited accounts. Where such accounts are not available, the ICO will consider the preceding year's accounts. However, the ICO states that it may choose to adjust the turnover figure to reflect the true scale of the undertaking, and use, for example, management accounts or forecast figures.

The starting point is adjusted by the following percentage based on the undertaking's turnover:

Annual turnover	***Range for adjustment***
Up to £2 million	Between 0.2% and 0.4%
Between £2 and £10 million	Between 0.4% and 2%
Between £10 and £50 million	Between 2% and 10%
Between £50 and £100 million	Between 10% and 20%
Between £100 and £250 million	Between 20% and 50%
Between £250 and £435 (or £437.5 for the higher maximum) million	Between 50% and 100%

No adjustment will be made for undertakings generating more than £435 million (or £437.5 million, as applicable) in annual turnover.

The ICO states that a higher turnover is likely to correspond to a higher percentage being applied in this step of the calculation; but the ranges are stated to be only indicative and the ICO retains the discretion to not account for turnover. The Guidance states that the ICO will give reasons for not making the adjustments in such cases.

CALCULATION

The calculation of the fine will follow the formula below where the statutory maximum is expressed as a fixed amount (e.g. where the undertaking's turnover is below £435 million or £437.5 million, as applicable):

the applicable fixed statutory maximum x adjustment for seriousness x turnover adjustment

Where the statutory maximum is expressed as a percentage of turnover (e.g. where the undertaking's turnover exceeds £435 million or £437.5 million, as applicable) the following formula will be used:

turnover x the applicable percentage statutory maximum x adjustment for seriousness

The above formulas determine the starting point of a fine. The ICO will then adjust the fine to reflect any aggravating or mitigating factors. The Guidance states that this will be done on a case-by-case basis; and this adjustment can result in the final fine being above or below the original starting range. The ICO expressly retains discretion to impose fines to the amount of the applicable statutory maximum.

As the last step, the ICO will adjust the sum to ensure that the fine is effective, proportionate, and dissuasive. This assessment considers both the combined amount of the fines and each fine individually, where multiple fines are given as a result of the same or linked processing operations; where the infringements stem from different conduct, the overall sum will not be assessed.

The ICO provides limited guidance as to what factors it will consider at this last stage. It highlights that the fine needs to dissuade both the undertaking against which an enforcement action is being taken and to generally deter other undertakings from breaching the UK Data Protection Law.

Given the brevity of the Guidance on this point, future practice of the ICO will prove important in providing clarity as to how the starting point of the fine will be adjusted.

FINANCIAL HARDSHIP

The ICO may reduce any fine in exceptional circumstances, where an undertaking may be unable to pay the fine due to their financial position. Financial hardship must be claimed during the investigation in order to be considered by the ICO. The ICO states that it will use this discretion only where the fine would irretrievably jeopardise an organisation's economic viability.

CONCLUSION

The Guidance does not suggest a significant departure from the previous fining practice of the ICO, at least in terms of the factors considered. However, it does provide greater clarity on the calculation process, allowing business to appreciate the likely (monetary) costs of non-compliance with the UK Data Protection Law by permitting them to calculate the starting point and likely ranges of a fine.

Given that the Guidance remains silent on certain points, the future enforcement practice of the ICO will be increasingly relevant to businesses under investigation.

AUTHORS

FOREIGN QUALIFIED LAWYER

LIVIA CREPALDI WOLF

FRANKFURT +49 69 7941 1176

LCREPALDI@MAYERBROWN.COM

PARTNER

ANA HADNES BRUDER

FRANKFURT +49 69 7941 1778

ABRUDER@MAYERBROWN.COM

ASSOCIATE

ONDREJ HAJDA

LONDON +44 20 3130 3096

OHAJDA@MAYERBROWN.COM

ASSOCIATE

ELLEN HEPWORTH

LONDON +44 20 3130 3953

EHEPWORTH@MAYERBROWN.COM

ASSOCIATE

ALASDAIR MAHER

LONDON +44 20 3130 3532

AMAHER@MAYERBROWN.COM

PARTNER

MARK A. PRINSLEY

LONDON +44 20 3130 3900

MPRINSLEY@MAYERBROWN.COM

ASSOCIATE

REECE RANDALL

LONDON +44 20 3130 3064

RRANDALL@MAYERBROWN.COM

PARTNER

OLIVER YAROS

LONDON +44 20 3130 3698

OYAROS@MAYERBROWN.COM