Browne Jacobson

Understanding the ICO's new fining guidance

19 April 2024

The Information Commissioner's Office (the ICO) has recently published new guidance for issuing fines for data protection breaches. It provides a detailed framework for determining the level of fines that should be issued, considering factors such as the severity of the breach, the number of people affected and the level of co-operation from the organisation in question.

The guidance also explains the legal framework that gives the ICO the power to impose fines, how the ICO will approach key questions such as identifying the wider 'undertaking' or economic entity of which the controller or processor forms part, and the methodology the ICO will use to calculate the appropriate amount of the fine.

The ICO is the UK's regulator for data protection and privacy, with the power to impose fines on organisations that violate data protection laws. The fines are designed to be a deterrent to organisations that fail to protect personal data, with the maximum fine for a serious breach being 4% of the organisation's global turnover or £17.5 million, whichever is greater.

What does the ICO's new fining guidance state?

The new guidance takes into account significant changes in the data protection landscape, including the introduction of the General Data Protection Regulation in 2018 (now known as the 'UK GDPR'). It introduces a two-stage process for determining fines, assessing the severity of the breach and the organisation's culpability.

The severity of the breach is assessed by considering the impact that the breach has had on individuals, while the organisation's culpability is assessed by considering factors such as the organisation's awareness of the breach, its compliance history and its level of responsibility for the breach.

The guidance also sets out a number of aggravating and mitigating factors that the ICO will take into account when determining the level of the fine. Aggravating factors include the organisation's failure to take appropriate technical and organisational measures to protect personal data, while mitigating factors include the organisation's prompt and effective action to mitigate the impact of the breach.

How much could an organisation be fined for breaching data protection?

The amount of the fine that the ICO can impose for an infringement of the UK GDPR is subject to a statutory maximum.

There are two levels of maximum fine – the standard maximum amount and the higher maximum amount, depending on the statutory provision that has been infringed. The maximum fine amounts for each level differ based on whether the controller or processor is an 'undertaking'.

The standard maximum amount is £8.7 million or 2% of the undertaking's total worldwide annual turnover, whichever is higher, while the higher maximum amount is £17.5 million or 4% of the undertaking's total worldwide annual turnover, whichever is higher.

The applicable statutory maximum amount is only calculated by reference to a percentage of turnover where an undertaking's total worldwide annual turnover exceeds certain thresholds.

What is the process by which the ICO issues fines?

The ICO can impose fines for a wide range of infringements under the UK GDPR and Data Protection Act 2018 and will assess each case individually before deciding whether to issue a penalty notice.

It will consider the seriousness of the infringement, any relevant aggravating or mitigating factors, and whether imposing a fine would be effective, proportionate, and dissuasive. The assessment is fact-specific and will depend on the circumstances of each individual case.

If the ICO decides to issue a penalty notice, the methodology for determining the fine amount will be applied. It may also require corrective measures in addition to or instead of a fine.

If it decides to issue a penalty notice, the fine amount will be calculated by applying a five-step approach:

1. Assess the seriousness of the infringement
2. Accounting for turnover (where the controller or processor is part of an undertaking)
3. Calculating the starting point, taking into account the seriousness of the infringement and, where relevant, the turnover of the undertaking
4. Adjust the fine amount to take into account any aggravating or mitigating factors
5. Assess whether the fine is effective, proportionate, and dissuasive.

What does the ICO’s new fining guidance mean for public bodies?

The new guidance has significant implications for businesses and other organisations.

It emphasises the importance of implementing effective data protection measures, and having a clear and effective breach response plan in place.

Non-compliance with the new guidance can result in significant fines and reputational damage. It is therefore essential that organisations take steps to protect personal data and comply with the new guidance.

The guidance also provides an opportunity for organisations to review their data protection measures and ensure they are up to date and effective.

By doing so, they can minimise the risk of fines and protect the personal data of both their customers and employees.

Summarising the ICO’s new fining guidance

In conclusion, the ICO's new fining guidance is an important development for public bodies.

It provides a detailed framework for determining the level of fines that should be issued for data protection breaches and emphasises the importance of implementing effective data protection measures.

Organisations must take data protection seriously and comply with the new guidance. Failure to do so can result in significant fines and reputational damage.

By implementing effective data protection measures, and having a clear and effective breach response plan in place, organisations can minimise the risk of fines and protect the personal data of their customers and employees.

Contact

Heather McKay

Senior Associate

heather.mckay@brownejacobson.com

+44 (0)330 045 2232

Related expertise

Data protection and higher education

Data protection and information sharing in academy schools and trusts

Data protection and privacy

Data protection for retail

Information law