10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

ICO consultation on draft Data Protection Fining Guidance

December 2023

About techUK

techUK is a membership organisation launched in 2013 to champion the technology sector and prepare and empower the UK for what comes next, delivering a better future for people, society, the economy and the planet.

It is the UK's leading technology membership organisation, with around 1,000 members spread across the UK. We are a network that enables our members to learn from each other and grow in a way which contributes to the country both socially and economically.

By working collaboratively with government and others, we provide expert guidance and insight for our members and stakeholders about how to prepare for the future, anticipate change and realise the positive potential of technology in a fast-moving world.

Introduction

The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018) establish a broad framework for handling personal data. The Information Commissioner's Office (ICO) plays a crucial role in enforcing these laws, with the authority to impose fines for serious breaches.

Proportionate fines are essential to encourage compliance without unduly burdening entities. Striking the right balance in fine calculation ensures that businesses, particularly those engaging in innovative and technology-driven ventures, can operate within a legal landscape that is both protective of individual rights and supportive of economic growth.

The ICO's recently published draft data protection fining guidance provides valuable clarity in this regard. However, we are of the view that it would be helpful to refine it further ensure that it aids the UK in establishing a data protection framework that aligns with the country's unique circumstances and aspirations. We set out our proposed changes below.

Defining the concept of 'undertaking'

The Information Commissioner's Office's (ICO) draft data protection fining guidance appears to have drawn heavily from the European Data Protection Board's (EDPB) guidelines and wider EU concepts. While this approach has its merits, it is crucial to ensure that the ICO's interpretation of "undertaking" aligns with the nuances of UK domestic law and the ICO's unique role in fostering economic development and innovation through effective regulation.

The UK's attractiveness as a destination for inward investment is well-established, with many organisations, from multinational corporations to small and medium-sized enterprises (SMEs) choosing to establish operations or invest resources within the country. These operations encompass a diverse range of activities, from providing core business services to specialised expertise in a variety of areas such as analytics, or cloud hosting.

The ICO's current definition of "undertaking" raises concerns that an entire organisation's revenue, regardless of its size, could be considered for relatively minor data processing infringements. This approach could have unintended consequences, potentially discouraging firms from utilising UK-based service providers or making bespoke investments in the UK.

To strike a balance between robust data protection and economic growth, the ICO should consider a more nuanced approach to determining the appropriate level of fines. Instead of relying solely on an organisation's global revenue, we are of the view that the ICO should carefully evaluate the specific facts and circumstances of each case, including the nature of the infringement, the scope of the data involved, the impact on individuals, and the size and resources of the organisation. Additionally, the ICO should prioritise considering the processing activity that occurred under UK jurisdiction during the infringement calculation and how it was isolated from the organisation's other activities that may not have been related to the infringement.

Furthermore, the ICO should exercise its discretion to set fines below the statutory maximum when appropriate. This would allow the ICO to tailor its enforcement actions to the specific circumstances of each case, ensuring that penalties are proportionate to the severity of the infringement and do not disproportionately impact scaling companies or stifle innovation.

By adopting a more nuanced and proportionate approach to determining fines and interpreting the concept of "undertaking," the ICO can effectively uphold its data protection mandate while fostering a thriving investment climate and a competitive business environment in the UK.

Taking a proportionate and clear approach to the calculation of fines

The draft guidance recommends that if a company violates multiple rules in the UK GDPR or DPA 2018 through connected processing activities, each violation can be fined separately. These individual fines can be combined, as long as the total does not go beyond the highest fine allowed for the most severe violation.

We are concerned that applying multiple fines for exactly the same breach and same conduct could be disproportionate. Therefore, we are of the view that the guidance should align with the principle of absorption, assessing the gravest infringement and determining a fitting fine for that single alleged violation.

Moreover, the guidance sets out that, where an organisation is found to have violated different rules under the UK GDPR or DPA, and these violations are not connected, the ICO might opt to group these infractions when imposing a penalty. Nevertheless, each violation would still be individually assessed against the maximum fine allowed by law. Consequently, the total fine could surpass the limit set for a single, most serious violation. In such cases, we recommend that the ICO, to determine the appropriate fine, should initially assess whether the rule violations are similar or different. To ensure fairness and transparency in this process, the guidelines should mandate the ICO to clearly articulate its reasoning on this matter.

Furthermore, the broad scope of the UK GDPR makes it challenging to establish fixed criteria for determining fines. We are of the view that the current guidance leaves too much discretion to the Information Commissioner, potentially leading to inconsistent and unfair penalties.

The Information Commissioner's Office should therefore adopt a more transparent and predictable approach to fining under the UK GDPR. This could be achieved by providing clear and comprehensive examples of the mitigating factors that will be taken into account when determining the extent of fines Additionally, clearly explaining how mitigating factors will be considered when determining the proposed fining ranges will ensure that organisations' compliance efforts are recognised. Similarly, offering concrete examples of breaches falling into each severity category will help organisations better understand the potential consequences of their actions. To enhance predictability, specific guidance on when

adjustments to fines will be made should be established. Finally, defining granular and objective criteria for determining fines, including specifying what constitutes a "serious infringement" and limiting turnover to UK-based turnover, will further promote fairness and consistency.

By implementing these recommendations, the ICO can foster a more predictable and fair fining system under the UK GDPR, encouraging organisations to prioritise compliance while maintaining a thriving business environment.