Executive Team – for discussion

Date: 10 Feb 2022
Prepared for: Executive Team

Topic: The application of corrective measures in the form of monetary penalties (fines) under UK GDPR to public authorities and bodies; which we take here to be those organisations covered in S3 of FOIA.

Issue: Consideration by ET of the desirability of commissioning work to amend our approach to fines on public sector organisations following a breach of data protection legislation.

Background:

1. Under the provisions of article 83 (and recitals) of the GDPR corrective measures, in the form of fines, may be applied by the supervisory authority. Article 83(7) GDPR also provides that national laws may be made with respect to whether public sector data controllers or processors should be subject to fines. EU countries have adopted a mix of approaches, with some countries allowing public sector fines and others removing the ability of the DPA to do so. The closest parallel is probably Ireland as they also have a common law system and fines are allowed with a cap of 1M euro.

2. GDPR reflects the general legal principle that fines should serve two purposes; 1) punish the infringement of the law in a proportionate and effective way and 2) deter further breaches of the law. The GDPR provides relevant factors at 83(2) that must be taken into account when deciding whether a fine should be applied, and, if so, at what level. These were mirrored across when GDPR became UK GDPR. DPA 2018 also makes the same provisions for law enforcement and intelligence service processing and introduces a fine for data controllers for failing to register with the ICO.

3. While the UK was in the European Union and subject to the Article 63 provisions of consistency, including through the one stop shop arrangement of the EDPB, the ICO faithfully reflected the GDPR considerations in its Regulatory Action Policy (RAP). This incorporated thinking from the EDPB's fines taskforce about the application and calculation of fines[1]. It additionally incorporated a consideration of 'affordability'. ICO consulted on its approach, received support for the

[1] https://ec.europa.eu/newsroom/article29/items/611237/en

approach, consulted SofS (DCMS) successfully and the approach was endorsed by Ministers and Parliament through the statutory consultation process. The UK issued 3 cases under the consistency mechanism using this approach; all were approved by the one stop shop. Two have settled with the penalty paid and one is subject to appeal. That will be the first tribunal appeal to our approach.

4. In introducing the GDPR (and then UK GDPR) the UK Government chose not to make any provision for exempting the application of GDPR fines applied to public sector organisations under GDPR A83(7). Arguably therefore it might be ultra vires to for the ICO to adopt a policy or guidance that expressly sets out a blanket position not to fine public sector organisations. Further work to confirm Parliament's rationale could be needed.

5. This follows a general UK approach of regulatory oversight including fines applicable to both commercial and public sector bodies where similar risks of harm arise. Often this is in the context of physical harm or safety considerations (e.g. Health and Safety Executive, Environment Agency, Driver and Vehicle Standards Agency, Care Quality Commission and others) and we could look in more detail at the way these are implemented if that would be helpful.

6. ICO has issued 20 fines over the past 5 years to public sector bodies. This represents approximately 7% of the penalties we have imposed. The UK public sector is estimated to comprise just under 40% of the UK economy in GDP terms.

7. Other DPAs have imposed GDPR penalties on public sector organisations[2], including:

    - Health authorities and hospitals in Italy;
    - Schools and universities in Sweden, Greece and Poland;
    - A police force in Cyprus; and
    - City administrations/regional or community authorities in Lithuania, Norway and Italy.

8. We have some flexibility now in how we apply an updated RAP and statutory guidance to address this issue. This paper explores options to do this while still maintaining effective data protection safeguards for UK residents. We are presently consulting on our RAP so there is scope to consider including any changes as part of that process. Under the policy, as a general principle, the more serious, high-impact, intentional, wilful, neglectful or repeated breaches can expect stronger regulatory action including fines. Breaches involving novel or invasive technology, or a high degree of intrusion into the privacy of individuals without having done a full Data Protection Impact Assessment and

[2] GDPR Fines Quarterly Report: Free Download (itgovernance.co.uk)

taken appropriate mitigating action and/or which should have been reported to the ICO but were not, can also expect to attract regulatory attention at the upper end of the scale.

Discussion:

9. It may be helpful to frame discussion by exploring different features of the issue:

Public Sector Configuration

10. The UK public sector is not a homogeneous group. Publicly owned and operated services may also undertake commercial activity and can earn significant commercial income running into many millions of pounds (e.g. hospital car parking charges, private healthcare services in NHS providers, sale of property or assets, investment income). This is often reflected in their CEO and senior staff pay and reward provisions. Revenue streams such as these are sometimes sat alongside either locally raised taxes (e.g. for the local police or fire service), subsidised fee income whereby a proportion of which is retained with the rest due back to the treasury or sponsor department (e.g. train fares), or by centrally raised taxation which is then distributed by the Treasury.

11. The sector also includes commercial entities providing public services under contract with central or local government and operating either in a local or national market or as monopoly providers for a contractual fee (e.g. NHS Blood and Transplant, elements of HM Coastguard, Social Care Homes, General Medical Practices, Dentists). Increasingly, large scale public services outside central government are headed by elected representatives and there is therefore some correlation between poor service / reputation and removal of the office holder (e.g. Police & Crime Commissioners, Metro Mayors for local health, transport and council services, Cabinet style government in local councils).

Dissuasiveness (Deterrence), effectiveness and proportionality

12. These are key tests for fines in the UK GDPR. A fine will often involve two factors; the reputational impact on the organisation (often in terms of the 'embarrassment') and its leadership and the impact on the service of the loss of funds (this latter factor may also involve reputation too if the loss of funds impacts the quality of the service itself). However, in practical fiscal terms, for public sector organisations directly funded by the treasury, a fine by the ICO might involve funds removed by the fine being reallocated to the organisation at a later date. As such there is a potentially weaker disincentive factor in those circumstances. In other, more locally

delivered, public sector organisations (where there is perhaps a component of commercial activity or a locally provided budget, for example through council tax charges) then there may be a stronger disincentive factor both in direct financial terms and also in terms of the reputational impact on the head of the organisation from either the fine itself, the deterioration in the service from there being fewer resources available, or because many of these services have a more direct link to local communities through elections or through deterioration of the organisations balance sheet that may attract board attention.

13. A fine can send a strong signal of regulatory disapproval by comparison with other sanctions (e.g. reprimand, even where these are publicised) if sufficiently tailored to the context of the sector. The ethos of public sector organisations can also mean that it is often a key driver that they try to 'do the right thing' and therefore they may be motivated already to seek to learn and avoid repetition of breaches anyway. Where it is picked up, a fine may also lead to wider deterrence across that specific area of the public sector as peers seek to avoid similar problems. This element of effectiveness will however differ depending on the configuration of the individual public service and the degree of communication activity that surrounds the fine as it requires peers to be aware of the incident. Again, in the more central services directly funded by the treasury this could be weaker as the revolving nature of the budget allocation and the more parochial interest in administrative matters could mitigate the impact of the fine (the 'wooden dollars' argument) and senior staff tend not to have direct performance measures based on regulatory compliance in central government

Equity concerns

14. Consideration might also need to be given to equity between different types of public sector providers and also the commercial sector. There are instances where public sector organisations are in direct competition with commercial entities (e.g. hospital day case surgery) and therefore a reduced compliance cost by not having fines could be seen to confer unfair competitive advantage. Anecdotal evidence (and a quick review of recent representations) is that the public / commercial comparison is not an often used argument at present however, albeit within sector comparison does feature and usually in terms of no-one wanting to be the highest fine (i.e "you fined our competitor X, you should fine us X-1 as we are not as bad as them?"). There could also be equity considerations in circumstances whereby central government public sector organisations were not fined because there was a lower incentive yet local public services are fined because there is a stronger local accountability incentive. These will need to be worked through if a change was proposed.

Types of fine

15. An area we may wish to explore too is whether we adopt a different stance to different types of fine. At present we can fine for:

    a. Failure to register and pay the fee
    b. Failure to report a breach to the ICO within 72hrs
    c. Failure to meet the substantive requirements of the UK GDPR
    d. Failure to comply with an ICO enforcement or information notice

16. We may want to consider therefore whether we adopt a different approach to these different types of fine. We might want to show more discretion on substantive matters but retain fines as an option for a failure to comply or co-operate with the ICO? Similarly we may wish to consider whether we should fine a public authority for not paying its DP fee but not to fine it for a data breach or failing to comply with an ICO notice or failing to co-operate with the ICO investigation? This could send an unintended message and could be misconstrued that we care more about our own revenue that the punishment of breaches?

Public interest / confidence and economic considerations

17. More analysis should be done as part of taking forward any work as we have little empirical information on views in relation to ICO fines[3]. In the mainstream, reporting of public sector fines in the past has been factual although some trade and the more specialist commentators do highlight the possible 'merry-go-round' nature of some of the financial flows in question. Most scrutiny of the fines does seem however to comment on the early payment discount of 20% more than whether a fine has been levied on a public body.

18. Another set of arguments in this space are around the public interest in imposing large penalties on public sector bodies, although fines are capped at app. £17.5m (unless the public sector body qualifies as an "undertaking" and generates turnover). Although our focus here is the public sector, it is worth noting that similar arguments also apply to any non-profit organisation, where recent examples from ICO enforcement include penalties imposed on charities (Mermaids, HIV Scotland), trade unions (Unite), and political parties (Conservative Party).

19. An argument is that imposing penalties on public sector organisations has the effect of reducing their ability to deliver their services in support of the public interest, and hence acts against the public interest. In basic economic terms this has some straightforward validity: assuming that revenues are (at least in the short term) fixed

[3] https://ico.org.uk/media/1042351/spa-future-thinking-report-slides.pdf

and there is zero profit, a penalty is a cost that must be met by reducing costs elsewhere, most obviously by not providing other services. This is a simple characterisation and we could question the assumption of finite revenues, for example where an organisation has multiple sources of income, generates a surplus or has reserves it could dip into, or could renegotiate its funding. In terms of incentives, while a public sector organisation might not care about profits, it will certainly care about costs that might inhibit its ability to deliver core public services (and not for profits will have a similar focus on their charitable objectives).

20. However the concept of 'public interest' is a wider interest than simply the provision of public services, as the ICO itself has explained in the context of DP. While imposing penalties might be to the detriment of public interest for the public service provision reasons set out above, it also has the offsetting effects of furthering the public interest in terms of 'protecting the public'. For example, as noted above penalties have a deterrent effect on other controllers (both public and private) which is likely to reduce future harms, and more generally raise awareness of DP issues both for controllers and the public. It could also be argued that there is public interest in greater awareness of personal data use in society, and its benefits and costs, enabling data subjects to make better informed choices, and in turn enabling competition and growth. Whilst not suggesting that this would lead to a net benefit to the public interest it is worth being aware that there are public interest arguments in both directions. It should be considered also that the public sector is responsible for considerable data holdings, including considerable volumes of highly sensitive personal data.

21. A more detailed analysis of our approach to fines is set out as an annexe for further reading if desired.

Options:

22. Several options may be worth considering:

a) We can choose to continue our present approach un-changed dealing with each case on its particular merits against the considerations set out in the UK GDPR and our RAP. In this we would continue to consider effectiveness, deterrence and proportionality as we go, but in future publish the factors that apply to public sector cases in our statutory guidance. In practice, this will mean that public authority fines will still be a possibility, but given the statutory cap likely at lower levels and less frequently than might be experienced in the commercial sector.

b) We can choose to use our discretion in how we regulate to focus on a more compliance / upstream approach to engagement with those we

regulate and emphasise more clearly the dissuasiveness and effectiveness components we consider in taking decisions about when to use fines. This could be in line with our recent discussions about how we approach cross-government thematic issues. If we are satisfied that the public sector body is aware and taking measures to address data protection risks then because of the potentially weaker disincentive factors for public bodies we may be content to advise and supervise rather than investigate and fine. Each case would need to be considered on its individual circumstances but this has opportunities in that it is consistent, keeps the option of a fine for wilful or reckless or negligent behaviours (or for failure to co-operate with ICO) and provides a strong 'backstop'. It has risks in that we need to ensure our work remains appropriately delivery focussed and independent, and we may want to develop transparent thresholds at which we transition from a compliance posture to considering a fine should we see harmful behaviours.

c) As an extension, or in concert with b), we could look at / focus on commercial revenue streams or other local sources of funding when making the affordability criteria assessment for public services and amend either the fine being applied or the level of the fine accordingly and amplify the proportionality and affordability tests to ensure these continue to provide the right incentive and drive incentives from the top of the organisation. This would have benefits in that the disincentive factor may still be felt by the senior decision makers in the organisation whilst not reducing to any great degree the public funds allocated to that particular public service. This has advantages in broad consistency with our present approach while allowing us to perhaps better explain / set out our considerations and the 'reasonableness' of our approach in this area when we do levy fines, and set out our desire to avoid detriment to public service users from regulatory action.

d) We can chose, subject to the further work set out above, to use discretion to not implement fines against public bodies and update our Regulatory Action Policy to reflect this. This could be a bold signal of change and could support a more compliance based posture for the public sector overall. It may however represent a risk that the ICO is acting unilaterally in an area where Ministers and Parliament have chosen not to make provision and could be open to challenge that ICO is developing policy itself and it might raise issues of lawfulness.

e) We can ask DCMS to consider and make provision exempting public bodies from ICO fines under the DP reforms or implementing a fine cap as in Ireland. This has advantages inasmuch as it would be consistent with the original A83(7) provision as well as allowing Parliament to consider the measure and would remove potential challenges from the commercial sector that we were disadvantaging

them. It has risks in that we would need to consider the fines for non-payment / registration should that lead to significant non compliance (unlikely but possible).

Recommendation

23. Although this paper is presented for discussion, and all options are possibility, option b (combined with c) might provide the best agility to react to the differing circumstances we see; retaining fines where they are stronger disincentives to the more harmful / willfully reckless behaviours while recognising that in other circumstances a more compliance focussed response may be more appropriate.

Next Steps:

24. If agreed, further work will be taken forward using the policy methodology and legal considerations to identify the exact changes we wish to make in our approach. Any changes can be worked up to be reflected in the next iteration of the regulatory action policy and statutory guidance which will be consulted with SofS and laid in Parliament or they can be raised with DCMS through the next phase of the DP reforms work, as is necessary.

Consultees: Director of Economic Analysis and Regulatory Portfolios, General Counsel, Deputy Commissioner (Regulatory Strategy).

Author: Deputy Commissioner (CRO)

Outcome reached: Preference is to take a compliance-based approach for public sector, focusing learning on rather than sanctions/penalties, for ~2 years. This should be explained in the RAP. Bring a further report to ET to give a work programme on messaging. Facilitate further discussion on RAP approach with ET at appropriate stage after feedback is received. There is a need to develop further comms and messaging to bust myths around public sector data sharing, inc. engagement with central gov.

Annexes

1. Paper from Economic Analysis team on administrative fines and incentives
2. Excerpt from statutory guidance for consultation setting out fines process

Annex 1 Paper from Economic Analysis team

ECONOMIC BRIEFING: THE EFFECTIVENESS OF REGULATORY PENALTIES

Introduction

The ICO's powers include the ability to impose monetary penalties where the laws that we regulate have been breached. These penalties aim to be "*effective, proportionate and dissuasive*" in the circumstances, ensuring they both punish organisations in breach and promote future compliance.[4]

This paper introduces some **economic concepts and thinking** that help to explain how regulatory penalties can meet these aims. The discussion draws on empirical and policy research that examines the economic rationale for penalties, including in a broader law enforcement sense and more specifically in regulation. The paper concludes by summing up how the economic concepts are consistent with how the ICO seeks to exercising its penalty setting powers.

Scarcity of regulatory resources

Modern economic thinking about regulatory compliance and enforcement owes much to the seminal work of Becker (1968), which considers law enforcement as an economic problem of the **allocation of scarce resources**.[5] Becker seeks to explain how optimal enforcement minimises the social losses caused by offenses. Importantly, these social losses include not only the damage caused by an offense, but also the resources required in investigating and in delivering enforcement.

Regulatory penalties as an effective deterrent

A key insight from Becker is that the **incentives of potential offenders** are driven both by the probability of being caught and the severity of punishment if detected and convicted. The intuitive consequences of this are that **dissuasiveness is enhanced by greater penalties**, as well as increased likelihood of detection and conviction.

Stigler (1970) extends this thinking, notably by introducing the idea of **marginal deterrence**.[6] In Becker's framework it is prohibitively expensive (and therefore suboptimal) to detect and punish all offences, but deterrence can be achieved simply by increasing penalties at no cost to the regulator. Stigler considers the incentives of a potential offender, using the example that if an offender will be executed for a minor assault and for murder there is no marginal deterrent to murder. Accordingly, while greater penalties are more dissuasive, **penalties must also be proportionate** to avoid creating perverse incentives to commit more harmful offenses.

Economic incentives for non-compliance

One of the implications of Becker's framework is that there is **economically rational non-compliance** with the law, where the costs of compliance exceed the expected costs of non-compliance. Factors that controllers would take into account when making a decision to comply include the costs of compliance, the risks of being caught and successfully enforced against, and the costs that any enforcement action creates (including monetary penalties, legal costs and reputational damage).

This thinking has been extended and applied in a wide range of contexts, including regulation. In a notable example, Harrington (1988) develops a model to seek to explain why the empirical evidence

---

[4] See: Statutory guidance on our regulatory action, pp. 19-20.
[5] See: Becker, G (1968) Crime and Punishment: an Economic Approach. Gary Becker won the 1992 Nobel Prize in Economics for his work to expand the domain of microeconomic analysis, including to the analysis of crime.
[6] See: Stigler, G (1970) The Optimum Enforcement of Laws. George Stigler won the 1982 Nobel Prize in Economics for work including analysis of the causes and effects of public regulation.

shows generally good compliance with environmental regulation despite limited surveillance and penalties.[7] He finds that **firms are highly likely to comply when the costs of doing so are low,** supporting a focus on reducing regulatory burdens to engender greater compliance. Harrington also observes that even when compliance costs are higher than potential regulatory fines, it's possible that **non-monetary factors also incentivise compliance**, such as reputational damage from poor publicity. To have this effect, regulators need to be adept at spotting breaches and communicating enforcement action effectively.

Harrington's findings are **reflected in general guidance on good regulation**. For example the OECD (2000) considers that explanations for regulatory non-compliance depend on the extents to which regulated entities:[8]

1. Know of and comprehend the rules;
2. Are willing to comply (whether because of economic incentives, good citizenship, acceptance of policy goals or enforcement pressure); and
3. Are able to comply with the rules.

It follows straightforwardly that compliance can be fostered by **improving understanding** of the law, and ensuring there are **incentives and ability** to comply.

Positive spillover effects from regulatory penalties

In economics, a scenario where an interaction between two parties impacts other parties not directly involved in the interaction is said to create an externality, or "spillover" effect. Research from Evans et al (2015) analyses how penalties handed down by an environmental regulator to non-compliant firm creates **positive spillover effects** for other firms.[9] The authors show that enforcement action strengthens the regulator's reputation, having a positive effect on compliance in other organisations. Penalties that can leverage spillover effects will therefore have a broader dissuasive effect, helping resource constrained regulators to achieve their priorities.

Positive spillover effects from regulatory penalties also have a positive impact on **economic growth and competition**. Enforcement, and the greater compliance that it fosters, mean that the interests of legitimate businesses are not harmed by being at a disadvantage to non-compliant firms. Removing this harm addresses **competitive distortions** and **disincentives to invest in compliance**, and aligns strongly with the ICO's economic growth duty.[10]

Conclusion

It is apparent from the discussion above that the ICO's existing approach for delivering "*effective, proportionate and dissuasive*" regulatory penalties is consistent with the underlying economic concepts and thinking. This includes seeking to:

- **Manage resource scarcity** by having clear regulatory priorities and focussing efforts where harm is greatest;
- Have a clear penalty-setting process that accounts for **economic incentives** and provides **proportionate dissuasive effects**; and

[7] See: Harrington, W (1988) Enforcement leverage when penalties are restricted (available on request).
[8] See: OECD (2000) Reducing the risk of policy failure: Challenges for regulatory compliance.
[9] See: Evans, M et al (2015) Enforcement spillovers: Lessons from strategic interactions in regulation and product markets.
[10] See: Growth Duty: Statutory Guidance (publishing.service.gov.uk), p. 4.

- Support enforcement **spillover effects** by communicating regulatory action effectively and building public awareness.

Annex 2 - Excerpt from statutory guidance for consultation setting out fines process

Penalty notices

What is a penalty notice?

A penalty notice is a formal document that we issue (under section 155 DPA 2018) when we intend to fine a person or organisation for a breach, or breaches, of the data protection legislation we regulate. The penalty notice sets out the amount we intend to fine a person or organisation and the reasons for our decision.

Why do we issue penalty notices?

Our aim in applying penalty notices is to ensure compliance with legislation and information rights obligations. To do this, penalties must provide an appropriate sanction for any breach of data protection legislation, as well as an effective and proportionate deterrent to future non-compliance.

What is the process?

If we believe it may be necessary to issue a penalty notice, we would first issue a notice of intent (NoI). This explains why we believe a penalty notice is necessary and sets out details of the proposed penalty.

When a person or organisation receives an NoI, they can make representations to us about the content of the NoI and the proposed penalty. We carefully consider all representations before making a decision on whether to issue a penalty notice and, if so, what the penalty notice should include. We provide a detailed description of how we decide on appropriate penalties below.

When would a penalty notice be appropriate?

You should read this section alongside the "Regulatory responsibilities" section of the RAP. When deciding whether it is appropriate to impose a penalty notice, the Commissioner has regard to the considerations set out in section 155 of the DPA 2018.

We assess whether a penalty is appropriate in each individual case on the basis of the particular facts. To help us to consider the appropriateness of any potential penalty, we take into account a number of factors including:

Aggravating factors

- the attitude and conduct of the person or organisation concerned suggests an intentional, wilful or negligent approach to compliance or an unlawful business or operating model;
- the breach or potential breach is particularly serious (for example, whether it involves any critical national infrastructure or service. Critical

national infrastructure includes buildings, networks and other necessary systems that provide essential public services, for example energy, finance, telecoms and water services);

- a high degree of damage to the public (which may include distress or embarrassment);
- the data protection legislation breaches resulted in a relatively low degree of harm, but it affected many people;
- the person or organisation significantly or repeatedly failed to follow the good practice set out in the codes of practice we are required to promote;
- the person or organisation did not follow relevant advice, warnings, consultation feedback, conditions or guidance from us or the data protection officer (for data protection cases);
- the person or organisation failed to comply with an information notice, an assessment notice or an enforcement notice;
- the breach concerns novel or invasive technology;
- in data protection cases, if the person or organisation is certified by an accredited body under Article 43 of the UK GDPR, and failed to follow an approved or statutory code of conduct;
- the person or organisation's prior regulatory history, including the pattern, number and type of complaints about the issue and whether the issue raises new or repeated concerns that technological security measures are not protecting the personal data;
- the vulnerability, if any, of the affected people, due to their age, disability or other protected characteristic under the Equality Act 2010 (or section 75 Northern Ireland Act 1998);
- the breach involves special category data or a high level of privacy intrusion;
- the state and nature of any protective or preventative measures and technology available, including by design;
- the way we found out about the breach or issue and, if relevant, failure or delay by the person or organisation to notify us of the breach or issue; and
- if the person or organisation, directly or indirectly, gained any financial (including budgetary) benefits or avoided any financial losses.

Mitigating factors

- if the person or organisation notified us of the breach or issue early and has been open with us;
- any action the person or organisation took to mitigate or minimise any damage (including delay) that people suffered;
- any early action the organisation took to ensure future compliance with a

relevant code of practice;

- in data protection cases, whether the person or organisation followed an approved or statutory code of conduct;
- the state and nature of any protective or preventative measures and technology available; and
- whether the person or organisation co-operated fully with us during any investigation.

Other factors we may consider

- the cost of measures to mitigate any risk, issue, or harm;
- the gravity and duration of a breach or potential breach;
- whether the person or organisation is representative of a sector or group, raising the possibility of similar issues arising again across that group or sector if they do not address them;
- any action the organisation took to report the breach to other appropriate bodies (such as the National Cyber Security Centre (NCSC)) and followed their advice;
- the public interest in taking regulatory action (for example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute); and
- whether another regulator, law enforcement body or competent authority is already taking (or has already taken) action over the same matter.

What if an organisation or person does not agree with the content of an NoI?

As noted above, before issuing a penalty, we issue an NoI that advises the person or organisation that we intend to serve them with a penalty. The NoI sets out:

- their name and address;
- our investigative findings and the reasons why the Commissioner proposes to give a penalty notice; and
- the proposed level of penalty and any relevant aggravating or mitigating factors.

We invite written representations from the person or organisation about any aspect of the NoI. We allow the person or organisation at least 21 calendar days to make these representations. We consider these representations prior to our final determination as to whether a penalty is appropriate and, if it is appropriate, the level of penalty that we impose.

If we consider that it is appropriate for a person or organisation to make oral representations about our intention to give a penalty notice, then the NoI would

state this. It would also specify the arrangements for making such representations and the time at which, or period within which, they may make them.

If a person or organisation thinks that their circumstances warrant oral representations, they can explain how they justify this extra step in their written representations. In particular, we need to understand what oral representations would add to the information that an organisation has already provided in writing. We then decide whether or not to invite the organisation or person to a face-to-face meeting.

Where we are required to make reasonable adjustments under the Equality Act 2010, we would permit oral representations without the organisation or person making prior written representations.

We may convene a panel in cases where we are considering a fine in excess of £5m or in circumstances where we believe any proposed penalty or regulatory action is likely to cause a very significant financial impact on the recipient's business model.

The role of the panel is to decide whether the proposed fine (or any corrective measures) are effective, proportionate and dissuasive, by considering:

- the evidence in the case;
- the relevant legislation;
- the recommendations of the penalty setting meeting to the Commissioner;
- whether the action is consistent in scale and scope with our previous regulatory action; and
- any representations from organisations regarding the NoI.

The panel then makes a recommendation about the appropriate range of the fine or other corrective measures which they consider to be appropriate. They write a brief report which sets out the reasons for the panel's recommendation. The Commissioner has the final decision about the level of penalty we apply.

Schedule 16 of the DPA 2018 sets out full details of the information a penalty notice includes. We also advise those subject to penalties of any relevant rights of appeal.

How do we calculate the level of any penalty we impose?

We base our approach to the calculation of administrative penalties on the considerations set out in sections 155 to 157 of the DPA 2018.

The way we calculate financial penalties is fair, consistent and takes all relevant evidence and representations into account before we reach our final decision. We

use a nine step process to help us to determine the level of any penalty, and we set this out in detail below.

The legislative caps

The law imposes clear upper limits for the level of any penalty. As set out in section 157(5)-157(6) of the DPA 2018, any penalty we impose cannot exceed the statutory maximum. The maximum amount (limit) of any penalty depends on the type of breach and whether the "standard maximum amount" (SMA) or "higher maximum amount" (HMA) applies, pursuant to s.157(2)-157(4) of the DPA 2018.

In the case of an undertaking, the standard maximum amount is £8,700,000 or 2% of turnover, whichever is higher. In any other case, the standard maximum amount is £8,700,000.

In the case of an undertaking, the higher maximum amount is £17,500,000 or 4% of turnover, whichever is higher. In any other case, the higher maximum amount is £17,500,000.

References to turnover in relation to penalty calculations is a reference to an undertaking's total annual worldwide turnover in the financial year which precedes the penalty calculation.

The level of penalty we impose within the above limits depends on the facts of the particular case. When determining the appropriate level, we ensure that the overall penalty sum is effective, proportionate and dissuasive. In determining this, we consider, in particular, the following factors:

- the nature, gravity and duration of the failure, taking into account the nature, scope or purpose of the processing concerned as well as the number of people affected and the level of damage they suffer;
- the intentional or negligent character of the failure;
- the degree of responsibility of the person or organisation in question, taking into account any technical or organisational measures they implemented;
- the organisation's turnover (in the event that they are undertakings) or the economic situation of any other person that we would impose a fine;
- any relevant previous failures by the person or organisation;
- the degree of co-operation with us in order to remedy the failure or mitigate its effects;
- the categories of personal data that the failure affected;
- whether the person or organisation notified us of the failure;
- the person or organisation's previous history of compliance with notices we issued;

- adherence to approved codes of conduct or approved certification mechanisms;
- any other aggravating or mitigating factors or, where applicable, both; and
- any sufficiently similar or relevant previous decisions by us and other data protection regulators.

Having calculated the penalty sum on the basis of these factors, we also consider the wider economic impact of imposing the penalty sum. We also apply any reductions for early payment (see below).

An appropriate person within the ICO determines the final decision on the amount of an administrative. Our scheme of delegations explains the decision-making powers our staff hold and which staff have the authority to make decisions regarding administrative penalties. You can find the scheme of delegations on our website.

The nine steps before making a recommendation on a penalty amount

For each case, we complete the following nine steps before we make our recommendation on the amount of an administrative penalty:

Step one	Assessment of seriousness considering relevant factors under section 155 DPA 2018.
Step two	Assessment of whether the failure was intentional or due to negligence.
Step three	Determination of turnover or equivalent (where applicable).
Step four	Calculation of an appropriate starting range.
Step five	Consideration of other relevant aggravating and mitigating features.
Step six	Consideration of ability to pay.
Step seven	Assessment of economic impact.
Step eight	Assessment of effectiveness, proportionality and dissuasiveness.
Step nine	Early payment reduction.

The considerations at each step are:

Step one: Assessment of seriousness considering relevant factors under section 155 DPA 2018

We start by considering the seriousness of the failure. We do this by taking into account sections 155 (3) (a), (c), (d), (e), (f), (g), (h), (i) and (j) of the DPA 2018 and Article 83(2) UK GDPR, specifically:

- the nature, gravity and duration of the failure, taking into account the nature, scope or purpose of the processing concerned as well as the number of people affected and the level of damage they suffered;
- any action the person or organisation took to mitigate the damage suffered by people;
- the degree of responsibility of the person or organisation, taking into account technical and organisational measures implemented by them in accordance with section 56, 66, 103 or 107; any relevant previous failures by the organisation or person;
- the degree of co-operation with us, in order to remedy the failure and mitigate the possible adverse effects of the failure;
- the categories of personal data that the failure affected;
- the way we found out about the breach, including whether, and if so to what extent, the person or organisation notified us of the failure;
- the extent to which the person or organisation complied with previous enforcement notices or penalty notices; and
- their adherence to approved codes of conduct or approved certification mechanisms.

We assess seriousness on a scale using levels of low, medium, high and very high. Possible examples for each level are as follows:

"low" seriousness:

- A minor infringement, short in duration with a low number of impacted people and where the affected data did not contain special category data or where people did not suffer any damage. The person or organisation fully complied with reporting requirements and has no relevant regulatory history.

"medium" seriousness:

- A moderate level infringement, short in duration with a limited number of affected people or where there is limited damage to members of the public. The person or organisation partially complied with reporting requirements and has no or little relevant regulatory history.

"high" seriousness:

- A serious infringement which occurred over a prolonged time period, with a high number of people affected or significant damage to the public involving, for example, special category data. The person or organisation reported the incident late and has some relevant regulatory history.

"very high" seriousness:

- A very serious infringement which occurred over a prolonged time period with a very high number of people affected or significant damage to the public involving, for example, special category data. The person or organisation failed to report the incident and has significant relevant regulatory history.

The above examples are general indicators only, and we will take into account all the relevant Article 83 considerations when making a decision as to seriousness.

Step two: Assessment of whether the failure was intentional or due to negligence

In accordance with section 155 (3) (b) DPA 2018 and Article 83 (b) UK GDPR, we also take into account the intentional or negligent character of the failure. This looks at specifically whether the person or organisation was intentional or negligent about their responsibility for the failure.

Intention involves knowledge and wilfulness. Examples of intentional failures might be unlawful processing authorised explicitly by the organisation's top management hierarchy, or in ignoring their DPO's advice.

We consider negligent failures to be those which are unintentional. This is where the person or organisation did not intend to cause the failure, but nevertheless they failed to comply with data protection law. Examples of negligent failures may be failure to:

- check for personal data in published information; or
- read and follow existing policies.

Step three: Determination of turnover or equivalent

Article 83(4)-83(5) UK GDPR and section 157 of DPA 2018 set out the maximum amount of a penalty that we may impose on an undertaking with reference to turnover. We also use turnover or equivalent to determine the starting range for a penalty (see step four) for undertakings and non-undertakings, to provide consistency and fairness in penalty setting.

To establish turnover or equivalent, we review the relevant financial information and obtain expert financial or accountancy advice if we require. Where necessary, we will ask for financial information to help us to understand the circumstances. Where there is a lack of co-operation in providing all relevant financial information, the panel may decide to rely on the information that is available, or otherwise give greater weight to the factors they consider in other steps of the process (such as aggravating features under step five).

Where the subject of a penalty is not commercial in nature and may not therefore have a turnover, we will consider equivalent information on the relevant financial circumstances, including income, budgets or expenditure.

We consider turnover to be a relevant consideration when settling upon a penalty amount which is dissuasive and proportionate, however it is not determinative. In certain circumstances, in order to be sufficiently dissuasive, we may need to set a relatively high penalty even where an undertaking has a comparatively low turnover, or no history of turnover.

We will determine the relevant undertaking by taking into account the circumstances of every case. We will primarily review the ownership structures of the entities involved to determine which form part of the undertaking. It may be that, for example, the data controller or processor is a subsidiary of a parent company and together they constitute a single economic unit and single undertaking. In those circumstances, where there is sufficient evidence, we will calculate the penalty with reference to the turnover of the undertaking as a whole rather than the turnover of the controller or processor concerned.

Step four: Calculation of an appropriate starting range

We determine a starting range for the calculation of the penalty as set out below. We base the starting range for the penalty on the seriousness of the breach, as evaluated at step one above. We will then apply the appropriate percentage to the turnover or equivalent as determined at step three. The starting point will be determined by taking into consideration the assessment of whether the failure was intentional or due to negligence, as determined at step two.

For infringements where the standard maximum amount (SMA) applies, we consider the following starting ranges to be appropriate:

- For infringements with a low-level of seriousness, an appropriate starting range would be 0-0.5% of turnover or equivalent.
- For infringements with a medium-level of seriousness, 0.5-1% is an appropriate starting range.

- For infringements of a high-level of seriousness, 1-1.5% is an appropriate starting range.
- For infringements of a very high-level of seriousness, 1.5-2% is an appropriate starting range.

In determining a starting point within that range, we consider whether the failure was intentional or due to negligence in the specific circumstances of the case. Those who have acted negligently can expect a lower starting point than those who have acted intentionally.

For infringements where the higher maximum amount (HMA) applies, we consider the following starting ranges to be appropriate:

- For infringements with a low-level of seriousness, an appropriate starting range would be 0-1% of turnover or equivalent.
- For infringements with a medium-level of seriousness, 1-2% is an appropriate starting range.
- For infringements of a high-level of seriousness, 2-3% is an appropriate starting range.
- For infringements of a very high-level of seriousness, 3-4% is an appropriate starting range.

In determining a starting point within that range, we consider whether the failure was intentional or due to negligence in the specific circumstances of the case. Those who have acted negligently can expect a lower starting point than those who have acted intentionally.

In determining the starting point of the penalty, we will use rounded figures.

Step five: Consideration of other relevant aggravating and mitigating features

In line with section 155 (3) (k) DPA 2018 and Article 83 (2) (k) UK GDPR, we consider any aggravating or mitigating factors which we have not already considered in previous steps. These include, where applicable, factors such as any financial benefits the organisation or person gained, or losses avoided from the breach (whether directly or indirectly).

When determining the amount of any proposed administrative fine, we adjust the starting point figure for each band accordingly, upwards or downwards, to reflect our considerations of the above. We clearly record which aggravating and mitigating features we take into account and why and how we consider that these features influence the proposed administrative penalty.

Step six: Consideration of ability to pay

Based on the information available, we consider the likelihood of the proposed recipient of the penalty being able to pay the proposed penalty and whether it may cause undue financial hardship. If required, we review or obtain expert financial or accountancy advice in support of this step.

This is particularly important if an organisation or person's ability to pay is unclear or they have had a recent change in their financial, trading or competitive status. We would ask the organisation or person for information about their ability to pay, as appropriate.

Should a claim of financial hardship be made, we will expect it to be supported by evidence including (but not limited to) historical financial statements and other information considered relevant, such as internal forecasts.

Step seven: Assessment of economic impact

We must consider the desirability of promoting economic growth when exercising our regulatory functions under the DPA 2018, in accordance with our duties under section 108 of the Deregulation Act 2015. As such, we must ensure that we only take regulatory action when we need to, and that any action we take is proportionate. We must take this into consideration whenever we exercise a specified regulatory function.

We therefore consider the impact of any proposed penalty on economic growth, both in terms of the impact on the intended recipient, and more broadly.

We may consider agreeing payment of monetary penalties in instalments. This would depend on the recipient showing, to our satisfaction, that there are economic, financial or other reasons, why this is necessary.

We would not make any agreement to allow payment in instalments where the payment would no longer be effective and dissuasive.

Step eight: Assessment of effectiveness, proportionality and dissuasiveness

We ensure that the amount of the fine we propose is effective, proportionate and dissuasive. We can adjust it accordingly, in line with section 155 (3) (l) DPA 2018 and Article 83 (1) UK GDPR.

We also confirm that the final level of penalty imposed complies with the applicable cap (as set out in the section above on legislative caps).

Where there are multiple linked infringements, we shall consider them together and calculate a total penalty which shall not exceed the applicable cap for the gravest infringement.

Step nine: Early payment reduction

We would reduce the monetary penalty by 20% if we receive full payment within 28 calendar days of sending the notice. This early payment reduction does not apply in circumstances where we agreed an instalment plan.