

A vertical bar on the left side of the text, composed of three stacked rectangular segments: a dark red top segment, a yellow middle segment, and a dark blue bottom segment.

Internal Audit Report
Fees and Income
September 2020



Contents

- 01 Introduction
- 02 Background
- 03 Key Findings
- 04 Areas for Further Improvement and Action Plan

Appendices

- A1 Audit Information

In the event of any questions arising from this report please contact Peter Cudlip, Partner (peter.cudlip@mazars.co.uk) or Darren Jones, Manager (darren.jones@mazars.co.uk).

Disclaimer

This report (“Report”) was prepared by Mazars LLP at the request of the Information Commissioners Office (ICO) and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, We have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of the Information Commissioners Office (ICO) and to the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk. Please refer to the Statement of Responsibility in Appendix A1 of this report for further information about responsibilities, limitations and confidentiality.

01 Introduction

As part of the agreed Internal Audit Plan for 2020/21, we have undertaken a review of the Information Commissioner's Office (ICO) arrangements for fees and income, with a primary focus on data protection fees. We have reviewed key elements within the fee income process to ascertain whether processes and controls are designed and operating effectively. This included risks in the following areas:

- Policies and Procedures;
- Roles and Responsibilities;
- External Guidance;
- Fee Payment;
- Unpaid Fees;
- Fee Allocation;
- Other Income; and
- Performance Monitoring.

Full details of the risks covered are included in **Appendix A1**.

We are grateful to the Director of Digital, IT and Business Services, Head of Business Services, Group Manager for Data Protection Fees and other ICO staff for their support during the course of this audit.

The report summarises the results of the internal audit work and, therefore, does not include all matters that came to our attention during the audit. Such matters have been discussed with the relevant staff.

The fieldwork for this audit was completed whilst government measures were in place in response to the coronavirus pandemic (Covid-19). The fieldwork for this audit has been completed and the agreed scope fully covered. Whilst we had to complete this audit remotely, we have been able to obtain all relevant documentation and/or review evidence via screen sharing functionality to enable us to complete the work

02 Background

ICO is the primary enforcement body in England and Wales for data protection business compliance and laws. Eligible businesses and organisations (unless exempt under Schedules 2 - 4 of the Data Protection Act 2018) are classified into three tiers based on their size, which in turn determines their data protection fee (£40, £60 or £2,900); this is payable on an annual basis. Some exemptions apply simply because you have a particular purpose. But others only apply to the extent that complying with the GDPR would:

- Be likely to prejudice your purpose (e.g. have a damaging or detrimental effect on what you are doing); or
- Prevent or seriously impair you from processing personal data in a way that is required or necessary for your purpose.

Organisations are not legally obligated to provide documentary evidence for exemptions. However, ICO will challenge organisations where they believe further clarification of the exemption is required.

Data protection fees account for 87-90% of ICO's income. In Q1 of the 2020/21 financial year, data protection fee income amounted to £11.1 million, approximately £800k ahead of projections despite the Covid-19 pandemic and consequential uncertainty for many smaller businesses. Where businesses are struggling financially as a result of Covid-19 these being monitored by ICO's Business Services Team, and followed up in due course to obtain fees where possible.

The data protection income process is managed internally via the ICE system. Fees are received via three methods: Direct Debit (56%), Card Payments (35%), Cheque (2%) and BACS Payments (7%).

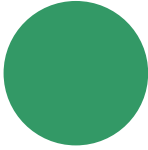
Unpaid fees are subjected to ICO's NOI procedure (Notice of Intent); this is then followed by penalty fees in addition to the original fee, for non-compliance. Where ICO is ultimately unsuccessful in obtaining outstanding fines and original fees, these are outsourced to debt collection agency,

Forbes. In 2019/20 8,980 NOIs were issued, with 52% in payment. Of the remaining 48%, approximately half were due to the NOI being cancelled by ICO, most often due to retrospective allocation of fees. The income from the NOI process amounted to £579,640. Where NOIs were unsuccessful, penalty notices were issued, recovering a further £93,000, composite of fees and penalties. A further £57,000 was recovered by Forbes, at a cost of approximately £17,000 to ICO.

There are currently 50,000 renewals due in July 2020. ICO are currently in the process of conducting campaigns to increase data protection registration and also to provide further guidance and support to SMEs. ICO have instigated a campaign utilising business data that is publicly available from Companies House. This is aimed at systematically identifying and contacting businesses not currently registered with ICO; this will increase fee income, whilst also seeking to improve data protection practices generally in England and Wales. In addition, the Business Services' SME Hub will implement a micro-site on ICO's website. This will provide accessible guidance, FAQs and document templates to SMEs; the primary aim is to increase the value for money associated with paying a data protection fee, whilst also increasing the legal compliance of small businesses.

The remaining income at ICO consists mainly in the form of Grant in Aid ('GIA'). This is provided by the Department for Digital, Culture, Media and Sport (DCMS), with further GIA funding from other government bodies such as the Cabinet Office. This equates to approximately £6 million annually and supports staff costs, as well as other ICO work such as Freedom of Information requests and processing. The GIA is drawn down monthly. ICO report financial performance to DCMS on a quarterly basis, in line with their own quarterly financial reviews. During Covid-19, the DCMS has paid all GIA to ICO in a lump sum, as well as authorising use of up to £1.8 million in cash reserves as a contingency plan.

03 Key Findings

Assurance on effectiveness of internal controls	
	Substantial Assurance
Rationale	
<p>For the internal audit work carried out (please see Appendix A1 for the detailed scope and definitions of the assurance ratings) we have provided substantial assurance.</p> <p>There is generally a sound control framework in place, though our work has indicated that one housekeeping recommendation detailed in Section 04.</p>	

Priority	Recommendations
1. (Fundamental)	-
2. (Significant)	-
3. (Housekeeping)	2
TOTAL	2

Areas of Strength

- Fee Payment - Data protection fees account for approximately 87-90% of ICO's income. In Q1 of the 2020/21 financial year, data protection fee income amounted to £11.1 million, approximately £800k ahead of projections despite the Covid-19 pandemic and consequential uncertainty for many smaller businesses. ICO actively seek to identify and engage with organisations that are not registered but who are eligible to pay a DP fee via their Companies House Campaign. Data is collected by sector, allowing ICO to identify those that may be more or less efficient at registering for DP fees. Growing the register will increase fee income opportunities, which may in-turn increase wider compliance with data protection and also potentially reduce the need for legal action due to non-payment or data breaches.
- Fee Allocation – Approximately 7% of ICO's DP fees are paid by BACS. At the time of the audit, only 3.7% of BACS payments had been unallocated; these are reviewed via daily bank reconciliations and matched against any remittance advice received by ICO. Ultimately, 100% allocation requires cooperation from organisations.
- Unpaid Fee Recovery - 8,980 NOIs were issued in 2019/20, with 51.7% resulting in payment. Of the remaining 48.3%, approximately half were due to the NOI being cancelled by ICO, most often due to retrospective allocation of fees, or insufficient evidence of data processing activities. The income from the NOI process amounted to £579,640. Where NOIs were unsuccessful, penalty notices were issued, recovering a further £93,000 of fees and penalties. A further £57,000 was recovered by Forbes, at a cost of approximately £17,000 to ICO. Whilst there is costs here, it is clear this is a last resort, and the amount recovered is greater than the cost, so provides an overall cost benefit to ICO.
- Other Income Monitoring – ICO maintain a Grant in Aid tracker, which is monitored quarterly in line with reporting to DCMS. ICO has mitigated any potential Cashflow issues during Covid-19 by agreeing all Grant in Aid to be paid upfront by DCMS. They have also successfully negotiated the ability to utilise £1.8 million in cash reserves should the

need arise, which can be balanced over several financial years. Stress testing of the Grant in Aid and the services supported is also performed, with two key aspects being staffing costs and FOI requests.

- Performance monitoring – Income is monitored through the monthly management accounts, and is also reported via weekly emails to the Accountable Officer, two Directors and Finance Staff. For 2019/20 the March 2020 year end management accounts noted that all income was £3.4 million in excess of budget, representing a 6.5% increase in income above budget. For 2020/21 ICO had budgeted for total income of £61.0 million, which represented a 14.0% increase on the prior budget and 8.4% increase on prior year outturn. Income as at May 2020 was forecast in line with budget. A monitoring dashboard is also produced on a weekly basis to track income. The weekly dashboard also includes statistics on the Companies House campaign. This shows that for the last 15 weeks to July between 30,000 and 50,000 companies were applying to register.

Risk Management

We have identified the following key risks monitored by Board, of relevance to this audit:

R46 – Our financial forecasts are inaccurate and we fail to accurately predict fee income and expenditure requirements.

We note that income in the prior year (2019/20) exceeded budget by £3.4 million, 6.5% in 2020/21, ICO's income forecast for Q1 exceeds their target by £800k. It should be noted that the income profile for the year has been altered for Covid-19 to receive 19.0%, 20.8%, 26.6% and 33.6% for each quarterly respectively.

We further note that there is an inherent risk around the accuracy of tiers for organisations, as ICO does not actively verify individual details. Given that the register holds approximately 735,000 paying organisations, and that ICO

has ambitions to expand the register, we understand that this is not a feasible task to perform on all organisations.

Value for Money

Value for Money is always an important factor in governmental organisations, as more scrutiny is placed on the spending of public sector organisations. As such, the Data Protection Fee Income process has several key VfM areas:

The Business Services Team was created in February 2020. A developing initiative by the team is the SME Service Hub - aimed at creating guidance and example essentials for SMEs, spreading awareness of data protection and also building and sustaining relationships with ICO. This move will hopefully help to demonstrate an enhanced service offering by ICO in exchange for the data protection fee, which can currently be viewed as merely a simple business tax.

ICO's website has a 'Fee Assessment Tool', which allows an organisation to identify whether they are eligible to pay a data protection fee, and whether they fall within tiers one, two or three. There is a facility to help organisations understand whether they should appoint a DPO (Data Protection Officer). The SME Hub will further expand on support of this nature, tailoring it to the understanding of smaller businesses.

The Companies House Campaign is aimed at systematically identifying and contacting organisations not currently registered with ICO; this will increase fee income, whilst also seeking to improve data protection practices generally in England and Wales. The Campaign, whilst delayed by Covid-19, has currently identified over 2 million organisations for contact.

Sector Comparison

Whilst the collection of data protection fees is a process unique to ICO, there are still several best practice areas in relation to income management:

- Effective allocation of fees to customer accounts to ensure efficiency and arrears processes are not carried out needlessly, where fees have already been paid but unallocated;
- Robust processes for obtaining outstanding fees. The use of standard methods, timeframes and letter by ICO to chase overdue fee will help reduce arrears levels;
- Routine performance monitoring to inform financial planning and budgeting; and
- Use of data to identify further DP fee income.

04 Areas for Further Improvement and Action

Definitions for the levels of recommendations used within our reports are included in **Appendix A1**.

We identified a number of areas where there is scope for improvement in the control environment. The matters arising have been discussed with management, to whom we have made recommendations. The recommendations are detailed in the management action plan below.

	Observation/Risk	Recommendation	Priority	Management Response	Timescale/ responsibility
4.1	<p>Data Protection Income Fee Policy</p> <p><i>Observation:</i> ICO does not currently have an overarching Data Protection Fee Income policy or supporting process map for the end to end lifecycle of fee collection. Process guidance is uploaded to ICON, the ICO staff portal, however these documents do not identify individual roles and responsibilities of key staff.</p> <p>A process map may help to visualise the end to end process, combat silo working, and direct staff as workloads increase and automation becomes a larger aspect of the Data Protection Fee Income process.</p> <p><i>Risk:</i> ICO staff are not aware of how to process fee income and such leads to inefficiencies or loss of income.</p>	<p>ICO should consider implementing a process map for the E2E Data Protection Fee lifecycle. This should be supported by guidance that outlines roles and responsibilities attributable to team members.</p>	3	<p>An end to end process map may help staff outside of DP Fees Team but all staff within the DP Fees teams have a very clear understanding of our roles and remit and how all the processes hang together. We have procedures for all processes. Therefore, I don't feel not having an end to end process map would lead to loss of income or inefficiencies by DP Fee staff. However, I can see the end to end process being useful outside the team and to new starters.</p>	<p>Q1 – 2021/22</p> <p>Director of Digital IT and Business Services</p>

	Observation/Risk	Recommendation	Priority	Management Response	Timescale/ responsibility
4.2	<p>Incorrect Fee Tier</p> <p><i>Observation:</i> During testing of fee income for July 2020, we noted 150 instances (of a potential 49,788) where the fee tiering was not aligned to the fee being paid. We were informed that this is due to organisations reassessing their fee eligibility and that the ICE system has not been updated to reflect this.</p> <p>We further noted that the Fee Assessment Tool on the ICO website relies on the correct information being input. It is therefore possible to purposely or mistakenly self-assess your organisation as eligible for a lower tier of fee. We understand that given the number of organisations that register and pay fees, and the checking this would involve by ICO, it is a risk that is accepted.</p> <p><i>Risk: ICO does not know all organisations that are required to pay a fee.</i></p>	<p>ICO should implement a data consistency check on a periodic basis to identify records that require updating.</p>	3	<p>For assurance we do routinely checks each time a company rings the helpline – during the conversation, we check their fee tier as a matter of course and make the tier changes if necessary. Last year, we moved lots of Tier 1 organisations to Tier 2 and some Tier 2 companies to Tier 3. We also have moved some companies from Tier 2 to Tier 1 and Tier 3 to Tier 2 or 1. Also, if we receive a written request for a change from a tier 3 to tier 2 or 1 or tier 1 or 2 to a tier 3 – these are checked as standard.</p> <p>We will implement an annual data consistency check in order to identify records that require updating. This will be completed following the end of the current financial year.</p>	<p>31 April 2021</p> <p>Director of Digital IT and Business Services</p>

A1 Audit Information

Review Control Schedule	
Client contacts:	Mike Fitzgerald, Director of Digital, IT and Business Services Faye Spencer, Head of Business Services Traci Shirley, Group Manager – Data protection Fees
Internal Audit Team:	Peter Cudlip, Partner Darren Jones, Manager Matt Bell, Internal Auditor
Exit Meeting:	23 July 2020
Last information received:	27 August 2020
Draft report issued:	14 September 2020
Management responses received:	25 September 2020
Final report issued:	30 September 2020

Scope and Objectives

Our audit considered the following risks relating to the area under review:

- Policy and Procedure – ICO does not have effective policies and procedures in place for income and fees
- Roles and Responsibilities – ICO does not have clearly defined roles and responsibilities that are aligned to the requirements of the policies and procedures
- External Guidance – ICO does not provide appropriate guidance to organisations to enable them to understand the DP fee requirements and make payments
- Fee Payment – ICO does not receive fees from all organisations that are required to pay a fee
- Unpaid Fees – Where fees are unpaid, ICO does not take any action to follow-up payment with the relevant organisations to receive payment
- Fee Allocation – Where fees are paid from an unknown source, ICO does not take appropriate action to determine the source of payment
- Other Income – Where other income is unpaid ICO does not take any action to follow-up payment with the relevant organisations to receive payment
- Performance Monitoring – Fee analysis is not undertaken on a regular basis and reported to the relevant group/committee.

The scope for the audit is concerned with assessing whether the ICO has in place adequate and appropriate policies, procedures and controls to manage the above risks. We will review the design of controls in place and, where appropriate, undertake audit testing of these to confirm compliance with controls, with a view to forming an opinion on the design of, compliance with and effectiveness of internal controls.

Testing will be performed on a sample basis, and as a result our work does not provide absolute assurance that material error, loss or fraud does not exist.

Assurance Level	Control Environment
Substantial	Findings indicate that on the whole, controls are satisfactory, although some good practice enhancements may have been recommended.
Adequate	While the control framework has been found to be generally well designed, control issues and / or areas for improvement have been identified. Where action is in progress to address these findings and any other issues known to management, these actions will be at too early a stage to allow a 'substantial' assurance audit opinion to be given.
Needs Improvement	Control weaknesses have been noted that require corrective action if the control framework is to be considered as operating effectively. Where such remedial action has already been identified by management, this is not currently considered to be sufficient, or sufficiently progressing to address the severity of the control weaknesses identified.
Limited	Findings indicate serious weaknesses in the control framework which could threaten the ability of the organisation to achieve its objectives; or, there is evidence that despite any corrective action already taken, key risks are crystallising in the area under review or have already crystallised. This assurance opinion may also cover the scenario where our audit work was obstructed such that we cannot conclude on the effectiveness of internal controls.

Definitions of Recommendations	
Priority	Description
1 (Critical)	Fundamental recommendations represent fundamental control weaknesses, which expose the organisation to a high degree of unnecessary risk.
2 (Highly Important)	Highly Important recommendations relate to matters which present some likelihood of seriously threatening the achievement of the organisation's strategic objectives.
3 (Significant)	Significant recommendations represent significant control weaknesses which expose the organisation to a moderate degree of unnecessary risk.
4 (Minor)	Minor recommendations show areas where we have highlighted opportunities to implement a good or better practice, to improve efficiency or further reduce exposure to risk.

Statement of Responsibility

We take responsibility to the Information Commissioner's Office (ICO) for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.