

Update since the Management Board meeting

Since the paper came to the Board a notification (registration) steering group led by Paul Arnold and Louise Byers has been established to direct the work reviewing current registration and fee paying arrangements. The group is producing a short business plan which will cover the following work streams:

- Research to understand the profile of the current public register – this has been commissioned and the supplier has started work.
- Research to estimate the number of registerable data controllers in the UK to give us an idea of how large the public register might be if we achieved close to full coverage - this will be delivered in-house once a new level D post in Registrations is filled. This post is being advertised.
- Application of research in order to forecast future fee levels based on expected size of the public register - as outlined in the paper.

The group will also be tasked with ensuring registrations are actively pursued to maximise the level of registration across data controllers. This includes:

- Work to introduce working practices to help us review all data controllers leaving the public register.
- Work to introduce ways of systematically identifying sectors to contact to raise awareness of the need to register and to establish efficient ways of doing this.
- Establishment of a proportionate referral mechanism of potential prosecution cases to be sent to Enforcement.

The group will also identify changes needed to ICE and the online registration service to support the work and develop business cases for change to be fed into the work of IT and Business Development.

Work to review the funding model with the Ministry of Justice is ongoing and will also be coordinated through the steering group.

Data Protection Fee Income – April 2015

Background

The upcoming European General Data Protection Regulation provides an opportunity to review the existing data protection fee arrangements.

The ICO has previously highlighted the need for an 'information rights fee' or one fee, paid by organisations directly to the ICO, to fund all information rights activities. Given concerns across government that this would result in private sector cross subsidising public sector work, the ICO recognises that this is unlikely in the short term.

As a result, the ICO's DP work will continue to be funded by fees from those it regulates, separate to the grant in aid funding it receives for FOI work. This paper sets out options as to how this mode may be changed and/or implemented differently to allow for more effective and efficient financial management and ensuring fee collection is fair and representative.

Legislative requirements

The Data Protection Act 1998 requires every data controller who is processing personal information to register with the ICO, unless they are exempt. The Act provides exemptions from notification for organisations that process personal data only for:

- staff administration (including payroll); advertising, marketing and public relations (in connection with their own business activity); and accounts and records;
- some not-for-profit organisations;
- organisations that process personal data only for maintaining a public register;
- organisations that do not process personal information on computer

Most organisations pay £35. The higher tier fee is £500, which is required to be paid if an organisation has a turnover of £25.9M and more than 249 members of staff or if they are a public authority with more than 249 members of staff.

At the year-end 2015/6, the ICO has around 409,000 data controllers registered, approximately 5,000 of which are higher tier fee payers. This equated to £17.4M data protection fee income.

Current issues

Forecasting DP income at the ICO has proved difficult due to nature of the fee, poor information systems and delays in processing. The new finance system, introduction of online payments including direct debit, BACS and credit card payments and process improvements in the notifications and finance teams have removed much of the issues within the ICO's control. However, fee income for 2014/5 was still £1.2m more than the original forecast. This creates uncertainty in budgeting and does not allow for accurate financial management.

In addition, some sectors have historically been under represented on the register. Although work has been done in the past to chase non notification, and this is one of the few circumstances where the ICO can prosecute for non-compliance, there has not been a significant push to ensure full, or close to full, registration. This is, in part, due to three factors – over recovery of income has to be remitted to the MOJ, a lack of resources in the non-notification area and because we have been unaware of what a full register should look like (despite undertaking some research in this area).

Changing the model – long term

We are currently working with the MOJ to review the current fee arrangements and consider how the model for fee income charging can be implemented. As part of this work, the ICO has set out some fundamental principles to the MOJ as to what a fee regime needs to achieve. These are aimed at informing at a high level what a new model needs to consider and include:

- Fees should be risk related and proportionate to the amount of time and resource the ICO requires to regulate certain organisations and sectors
- The fee structure needs to be flexible enough to change in both the risk profile (for example if new technologies or usage of data emerges) or for legislative changes (for example the new EU DP Regulation or EU case law)
- The fee needs to be easy for the ICO and stakeholders to understand. Too much complexity in the fee structure will mean that organisations cannot easily self-categorise, resulting in the risk of under or over payment, ICO resources spent checking and chasing organisations and uncertainty in fee income forecasting
- Exemptions, for example for domestic use; third sector or charities, should be clearly stated and well defined
- The fee does not need to be linked to registration but needs to be collected easily, for example online payments

- The fee needs to give the ICO surety of income and should allow for the fee to be flexed if more income is generated than is required in a year

Work so far with the MOJ has indicated a common understanding that the ICO should continue to collect fees using a tiered fee structure, but the tiers are changed to reflect more granular data protection risk. Initial analysis by MOJ suggested four tiers, based on the size of the organisation (for example based on number of employees or budget/turnover) and the amount of personal data processed (for example based on the number of data subjects or number of CCTV cameras.)

There is more work to do to establish how these factors then impact on how they use the ICOs services and how easy it is for organisations to collate the information they would need to categorise on either factor. Research is currently being commissioned to look at these issues.

Implementing the current model – short term

This work to review the way fees are charged will inevitably take some time to complete, and will require approval from Ministers and change in legislation. Therefore, the ICO needs to consider how the current model could be implemented differently.

Setting a stretching 'target' for fee income would allow the ICO to:

- Ensure a fairer representation of fee paying organisations
- Commit to longer term financial planning, including increasing head count, rather than shorter term cash spending in year
- Provide a sounder basis for making strategic decisions

There are risks associated with setting a 'target'. In particular, coming in under target may leave the ICO financial exposed. However, the income will be closely monitored throughout the year by the Financial Steering Group. There are also areas of spend which are discretionary and are back end loaded and could be revised if required. Conversely, if the ICO comes in over target this will still mean the ICO has not spent all DP fees on DP projects. This should also be clear early enough in the year through monitoring from the Finance Steering Group to mitigate in the year.

There may be concerns about setting a 'target' and how this fits with our regulatory responsibilities. However, ensuring all organisations who are data controllers are registered is provided for in the DPA.

To achieve this, a number of changes to current ways of working are required, some of which are already in process. The non-notification team is being expanded and roles are to be recruited to. External research is to

be commissioned to give a more accurate picture of what numbers of registered data controllers should look like.

In 2014/5 £17.5m was collected in fee income. In 2015/6, the ICO could set a target of between £18m and £19m and budget to spend this on additional staff in the first instance. This target could be revised on an annual basis and, for example, when the impact on the structure and staffing of the ICO resulting from the new EU DP Regulation, a revised target could be set.

Next Steps

Calculate how many organisations process personal data and therefore how many need to be registered. (A).

This is fraught with difficulty.

- There is no definitive list of businesses.
- Even within established categories, it isn't always possible to identify how many process data and need to notify.
- Businesses are constantly in flux, changing names, going out of business, merging etc.

Nevertheless, we should be able to come up with a figure that gives us an overall level of confidence of over 80%. We may have greater confidence in its accuracy in some areas than others.

Calculate what percentage of these organisations we can realistically expect to be registered. (B).

We could say that we require full compliance ie every organisation of any kind who should be registered must be. Full registration is a laudable stated aim and could be our strategic objective, but isn't ever going to be practical when new businesses are setting up all the time, when they change what they do or simply forget to renew.

We should therefore agree a percentage of the figure of organisations that need to register that we think will be registered each year. This needn't be a global figure. For example it could be 100% for elected representatives, 95% for law firms and a lower figure for general business.

We need to calculate how many organisation we expect to register. This will be B% of A. (C).

We need to calculate how much we need to spend in order to discharge our DP functions. (D).

This means looking at what we are doing and what we need to do and attaching a budget to it. This figure will need to be justified and agreed based on existing and known future functions.

Calculate how much we should be charging each data controller.

This will be based on D divided by C, but will have to be refined depending on the fee structure ie to take into account varying fees.

The fee(s) can then be set.

The ICO would monitor fee income as outlined above. As we prepared for the next year's budget, we could do the exercise again, looking at actual expenditure and factoring any projected over or underspend into the calculation.

Although there are a lot of complications in getting some of the figures, the actual calculation is straightforward.

The fee needn't be changed annually, it might be better to set a fee for two or three years and then adjust. This would only work if we were able to carry money forward from one year to the next.

Pros

It sets a fee that is fair, it gives the ICO ability to budget well in advance and help us manage our finances better.

Cons

The fee would change more frequently than under the current system, it requires good evidence in areas where we currently don't have much certainty (eg potential numbers to register), it would require additional resources to monitor, collect and enforce non-payment of fees (although these would be factored in to the budget).

Recommendation

1. It is too late to do this work for 2015/2016, so we should set a target for data protection income the year 2015/6 of £18m (based on 2014/2015 receipts plus approx. 3% anticipated increase).
2. Ensure budget lines, in particular in relation to recruitment and staff costs, are reviewed in light of expected income
3. Closely monitor income through the Finance Steering Group
4. Begin the next steps work referred to above leading to a budget for 2016/2017 by November 2015 (including proposals for fees).
5. Recruit additional resource to the non-notification team, using existing data and the outcomes of commissioned research to target under represented sectors.
6. Work with MOJ to develop a new funding model taking account of the principles outlined by ICO and the outcomes of commissioned research on the characteristics of data controllers

