

Committee of Public Accounts

Financial Statements 2018

Office of the Data Protection Commissioner (1 January – 24 May 2018)

Data Protection Commission (25 May – 31 December 2018)

[Subhead of Vote 24: Department of Justice and Equality]

Opening Statement of the Data Protection Commission

Chairman and Committee Members, thank you for the opportunity to address this Committee on the 2018 financial statements of the Office of the Data Protection Commissioner and the Data Protection Commission.

I am joined today by a number of my colleagues from the Data Protection Commission – which I will refer to from now on as the “DPC”. These are Deputy Commissioners Anna Morgan, John O’Dwyer and Graham Doyle and the DPC’s professional accountant Graham Geoghegan, who is a welcome new addition to our team in 2019.

The Data Protection Commission is fully funded by the Exchequer currently through a subhead of Vote 24 of the Department of Justice and Equality. This latter arrangement will change in 2020 when the DPC is to be allocated its own individual Vote at which point I, as currently the sole Commissioner for Data Protection, will become the Accounting Officer in line with Section 25 of the 2018 Act. In this context, the DPC appreciates this early opportunity to engage with the Committee as it will provide useful direction in terms of an exploration of the accounts of the DPC, particularly as the budget allocation to the DPC has increased considerably and as the authority now takes on many additional new and direct responsibilities in the areas of accounting, HR, ICT and procurement.

Role of the DPC

The Committee is aware that the DPC is the national independent supervisory authority responsible for monitoring and enforcing the application of EU data protection law. The General Data Protection Regulation or “GDPR”, the e-Privacy Regulations, the Irish Data Protection Acts 1988 to 2018, and the “Law Enforcement Directive” (transposed into Irish law as part of the 2018 Act), provide the main legal frameworks under which the DPC regulates. There are additionally in the region of 20 other pieces of legislation where the DPC must perform a particular supervisory function assigned to it. The Credit Reporting Act 2013 is one such example.

The provision that the data protection authority in each EU member state is independent in the performance of its functions is fundamental to the GDPR. Article 52 of the GDPR prescribes that each Member State shall ensure that the supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers. Currently, based on figures produced by the European Data Protection Board, the DPC in 2018 was the eighth largest in the EU in terms of both employee numbers and budget, slotting in behind, for example, the UK with 513 staff and a 2018 budget of over €51m and France with 199 staff and a budget of over €17m.

The Irish DPC operates in a very specific context at an EU level in that it is the “Lead Supervisory Authority” in the EU under the GDPR for most of the world’s largest technology companies given their headquarter locations here in Ireland. This brings considerable additional volumes of work, complexity and scrutiny but also grants the privilege to the DPC of handling cutting-edge cases in this important area of law.

2018 - a historic year of change in data protection

In terms of 2018, it is worth recalling at this point that it was a historic year in terms of data protection. The 2018 Act was the first comprehensive piece of national data protection legislation enacted in the State since 2003 and it gave further effect to the GDPR and transposed the Law Enforcement Directive in Ireland.

The core functions of the DPC, under the GDPR and the 2018 Act include:

1. **Handling complaints from individuals in relation to potential infringements of their data protection rights.** 4,113 complaints were received in the 2018 calendar year representing a 56% increase on the total number of complaints (2,642) received in 2017. 3,366 complaints were concluded in 2018. Some complaints are easily resolved with intervention by the Irish DPC. For example, an organisation may fail to provide an individual with a copy of their personal data and when the DPC intervenes, the data may then be immediately forthcoming. Other cases can be far lengthier and complex particularly where many different laws are in play. This has been particularly the case with complaints in relation to receiverships and liquidations, and in relation to cases involving disputes between employers and employees.

2. **Conducting inquiries and investigations regarding potential infringements of data protection legislation and enforcing the law as required using corrective measures and administrative fines.** In 2018, large scale investigations that were underway included the investigation into the Public Services Card, a finalised report and findings into non-compliance by the hospitals sector, 32 investigations into surveillance of citizens by the state sector through the use of technologies such as CCTV, body worn cameras, automatic number plate recognition (ANPR) enabled systems, drones and other technologies and 15 investigations of a range of issues concerning “big tech” companies. A final report and set of directions for compliance were also issued to Yahoo! EMEA Ltd (now known as Oath) in respect of infringements relating to what was at the time the largest data breach ever notified globally (500 million users affected). Further, the DPC in 2018 issued a significant decision against NAMA in relation to access to personal data and details of this decision feature in the DPC Annual Report (No. 1) for 2018. There were also 9 sets of District Court prosecutions taken by the DPC which concluded during 2018. 8 of these concluded successfully with costs awarded to the DPC and the final case was withdrawn due to compliance by the data controller (with an enforcement order).
3. **Promoting awareness among organisations and the public of risks, rules, safeguards and rights in relation to processing of personal data.** Over 50,000 contacts by email, telephone and web forms were received through the DPC’s Information and Assessment Unit. A number of campaigns via the DPC website and in the national media ran in 2018 to drive readiness for GDPR which included the launch of a comprehensive public consultation on children’s data. By the end of the awareness campaigns the DPC ran in 2018, 80% of Irish adults had been reached and 90% of SMEs, based on an independent survey commissioned by the DPC in March 2018, were aware of the GDPR. The increase in contacts with the DPC is continuing in 2019 with almost 50,000 received to date this year.
4. **Cooperating with data protection authorities in other EU member states on issues such as complaints and alleged infringements involving multinationals.** Over 80 European Data Protection Board meetings were attended in Brussels by DPC staff in 2018. As of last year, EU data protection authorities use a shared IT platform to transfer and exchange information on cases and over one third of the cases on this “IMI” (Internal Market Information system) platform were assigned to the Irish DPC in accordance with the rules of “One-Stop-Shop”. Delivery of a harmonised implementation of the GDPR across the EU is central to the aims of the new law.
5. **Assessing breach notifications from organisations that have a mandatory obligation to report to the DPC and ensuring mitigation actions have been taken.** 4,740 valid data security breaches were notified in the 2018 calendar year representing a 70% increase on the total number of valid data breaches (2,795) recorded in 2017. Each of these breach notifications was individually assessed and engagement with the reporting organisation took place, giving the DPC an opportunity to make recommendations in relation to procedural and security mitigation measures to be put in place.

Funding

The funding of the DPC by government has increased significantly in recent years from €1.7 million in 2013 to €11.7 million in 2018, which comprised an allocation of €7.3 million for pay and €4.4 million for non-pay expenditure. The allocation was further increased for 2019 with a total allocation of €15.28 million (€8.916 million for pay and €6.364 million for non-pay). This commitment of additional budget has allowed the DPC to grow its staff from 27 in 2014 to 110 at the end of 2018 and now 138 today.

The majority of expenditure at the DPC relates then to salary costs. The outturn on salaries for 2018 was €4.767million. During 2018, the DPC added an additional 25 staff, all of whom were recruited through specialist competitive recruitment campaigns to ensure the DPC has the legal, technological and investigative staff it requires to deliver on its mandate.

The DPC non-pay expenditure outturn was €3.286m and was comprised mainly of office accommodation costs, communications costs, legal fees and costs and business advisory services to prepare the DPC for GDPR.

Legal fees and costs represent the biggest category of non-pay expenditure and such cases will continue be a feature of the work of the Irish DPC, particularly now as punitive fines and measures can be imposed against organisations. Irish law allows a right of appeal by affected parties against decisions of the DPC. Currently the DPC has 24 live civil litigation cases active in the Courts. In addition, the DPC initiated what has been one of the most significant data protection cases in the EU when it brought a High Court application in May 2016 seeking a reference to the Court of Justice of the European Union (CJEU) on the validity of an EU legal instrument underpinning personal data transfers in a case involving Facebook and Max Schrems, a data protection activist. The case is of fundamental importance to the determination of core issues of data protection under EU law and has drawn global media coverage and worldwide interest far beyond the data protection community. The outcome of the case will potentially have worldwide ramifications for data transfers out of the EU and is being closely followed by data protection regulators, law makers and the data protection community. A decision of the CJEU is awaited in late 2019 or early 2020.

I hope I can assist the Committee further with responses to any questions you may have.

Thank you, Chairman.