

Corporate Governance Assurance Agreement 2017 -2019
between the Office of the Data Protection Commissioner and
the Department of Justice and Equality

1. Introduction

This Corporate Governance Assurance Agreement has been drawn up by the Department of Justice and Equality in consultation with the Office of the Data Protection Commissioner (DPC). It sets out the broad corporate governance framework within which the office of the Data Protection Commissioner will operate and defines key roles and responsibilities which underpin the relationship between the Office and the Department of Justice and Equality. While this document does not confer any legal powers or responsibilities, it forms a key part of the overall governance framework. The Agreement does not in any way impinge upon the absolute independence of the Data Protection Commissioner under the provisions of the Data Protection Acts 1988 and 2003, and the General Data Protection Regulation with effect from 25 May 2018. The purpose of the Agreement is to provide a framework for the administrative accountability of the office of the Data Protection Commissioner as a body funded by the exchequer.

Any question regarding the interpretation of this document shall be determined in consultation and agreement between the Minister/Department and the Data Protection Commissioner. It should be noted that the relevant legislative provisions will, of course, take precedence over any part of this document.

The independence of the DPC will be interpreted consistent with EU Directive 95/46 on the protection of personal data into national law as transposed into Irish law by the Data Protection Act 2003, the jurisprudence of the European Court of Justice and the Article 52 of the General Data Protection Regulation which will have force of law from 25th May 2018.

This document will be updated as necessary, and at least every three years.

1.1 As set out in the Data Protection Acts 1988 and 2003, the Data Protection Commissioner is a body corporate and is independent in the performance of her functions. The Data

Protection Commissioner is appointed by Government in accordance with the provisions of the Data Protection Acts.

- 1.2** The Data Protection Commissioner is responsible for upholding the EU fundamental right of individuals to have their personal data protected, in accordance with the provisions of the Data Protection Acts. The functions of the DPC include enforcing Data Controller compliance with Data Protection obligations, awareness raising and dealing with the complaints made by Individuals who feel their rights are being infringed.
- 1.3** The Data Protection Amendment Act, 2003, transposed the provisions of EU Directive 95/46 on the protection of personal data into national law. The Directive in providing for common minimum data protection standards for the European Economic Area required the establishment in each Member State of an independent authority to oversee implementation of the principles laid down in the Directive.
- 1.4** EU Directive 95/46 will be superseded by a new EU data protection framework comprising a General Data Protection Regulation (GDPR) and a Law Enforcement Directive. The GDPR as a Regulation will have direct effect, with the exception of a small number of limited areas where national discretion is allowed, will come into effect from 25 May 2018. The GDPR places significantly greater obligations and responsibilities on the DPC as an independent Supervisory Authority. For the first time the DPC will have the capability to impose administrative fines up to a maximum of €20m or 4% of global turnover for infringements of the Regulation. The GDPR also provides for a "one stop shop" mechanism for multinationals which will place Ireland as the lead EU regulator for all of the large Internet companies based in Ireland.

The draft EU Regulation on Privacy and Electronic Communications published by the EU Commission on 10 January 2017 proposes further additional and significant changes to the law aimed at enhancing the security and confidentiality of individuals' online

activities, including email and internet based instant messaging. As provided in the draft Regulation, the DPC as the independent national supervisory body responsible for monitoring and enforcing the application of the GDPR will also be responsible for enforcing the new ePrivacy rules.

The DPC has received additional funding and resources in 2015 and 2016 to assist in its preparation for the implementation of the GDPR, with further resources allocated for 2017. However, further additional resources will be required in 2018 onwards to ensure the DPC has the necessary resources to fulfil its responsibilities both under the GDPR and the proposed Regulation on Privacy and Electronic Communications.

- 1.5 The DPC was first established in 1989 in Dublin, and relocated to Portarlinton, Co Laois in 2005 under a government decentralisation programme. A Dublin office was re-established in 2015 implementing a Government decision in 2014 to establish an office in Dublin along with the provision of additional funding and staff resources.
- 1.6 The increase in the DPC's budget in 2015 and 2016 has facilitated the recruitment of additional staff, including legal, technical, audit and investigations specialists as well as policy and administrative staff. The 2017 budget allocation to the DPC of €7.5m will facilitate the ongoing recruitment of staff working towards the number of staff required by the DPC to perform its functions effectively. The overall sanctioned DPC headcount now stands at 62.
- 1.7 The purpose of this Agreement is to set out the arrangements for the effective governance, financing and general administration of the Office in accordance with the Code of Practice for the Governance of State Bodies (2016).

2. Role of the DPC within the Justice & Equality Sector

2.1 Mission

The DPC's mission, as outlined in its Strategy Statement (2014-16) is to protect the individual's EU fundamental right to data privacy by enabling people to know, and to exercise control over, how their personal information is used, in accordance with the Data Protection Acts and related legislation. The key principle underpinning data protection is that individuals should be able to control how information about them is used – or, at the very least, to be aware of how this information is used by others in accordance with the law.

2.2 Function

The core function of the Data Protection Commissioner is upholding the rights of individuals, as set out in the Data Protection Acts, and enforcing Data Controller compliance with their obligations under the Acts.

2.3 Objectives

The strategic objectives of the Office of the Data Protection Commissioner in support of its Mission are:

- To vindicate the individual's right to protection of personal data as laid down by law.
- To maximise levels of awareness and compliance with data protection obligations among those collecting and processing personal data.
- To provide timely, practical and easily understood guidance to individuals and organisations.
- To ensure that the individual's right to protection of their personal data forms part of the strategy for the more efficient delivery of public services, including public security.
- To carry out its activities in a cost-effective manner, making maximum use of technology and shared services, working cooperatively with other regulators and avoiding the imposition of unnecessary regulatory burdens on organisations.

- To prepare for the implementation of the GDPR and the proposed ePrivacy Regulation, ensuring that the DPC functions effectively in fulfilling its mandate under the new regulatory environment.

3. Corporate Governance

3.1 Roles and Responsibilities

Accounting Officer

The DPC falls under the Department of Justice and Equality's Vote (Vote 24) and as such the Department's Secretary General is the Accounting Officer. Further external scrutiny and governance is provided through the submission and analysis of the Appropriation Accounts to the Comptroller and Auditor General and ultimately to the Oireachtas through the Public Accounts Committee.

The Data Protection Commissioner

The Data Protection Commissioner is appointed by Government and is independent in the exercise of her functions. The Commissioner is responsible for upholding the rights of individuals as set out in the Acts, and enforcing the obligations upon data controllers. The Commissioner makes an annual report to the Oireachtas. The Commissioner's term is for a period of 5 years. The Commissioner can be removed from office if in the opinion of the Government she is incapable of performing her functions through ill-health or has stated misbehaviour. The Commissioner and her office are subject to the Code of Practice for the Governance of State Bodies.

The Office of the Data Protection Commissioner is staffed by civil servants who are bound by the Service Code of Standards and Behaviours, as well as corporate policies, procedures, circulars

and Office Notices insofar as they relate to the corporate governance and general administration of the office.

The Commissioner and her office are responsible for:

- The consideration and investigation of complaints from individuals who deem their data protection rights to have been breached by either public or private sector entities.
- The enforcement of the Data Protection legislation, as appropriate, against data controllers which contravene the Acts.
- The provision of guidance in relation to the application of data protection legislation.
- Coordination of its activities as necessary with other EU Data Protection Authorities (DPAs), both bilaterally and through the “Article 29” Working Party established under Directive 95/46/EC.
- The general administration and business of the office.
- The performance of any other functions as may be required by the Office.

3.2 Statement of Strategy

The DPC should regularly adopt a statement of strategy for a period of 3-5 years ahead. The DPC’s Strategy Statement 2014-2016 is available on its website, www.dataprotection.ie. Work is currently underway on the development of a new Strategy Statement.

3.3 Draft Unaudited Financial Statements

Draft unaudited annual financial statements should be submitted to the Department not later than two months after the end of the relevant financial year, in accordance with the *Code of Practice for the Governance of State Bodies* (1.4 (ii) – ‘Business and Financial Reporting’ Annex).

3.4 Annual Report

Section 14 of the Data Protection Act 1988 requires the DPC to make a report to the Minister for Justice and Equality (“the Minister”) each year, in relation to the performance of the functions and activities of the DPC during the preceding year. Copies of the report are required to be laid before the Houses of the Oireachtas.

3.5 Accounts

Section 9, Schedule 2 of the Act provides that the Commissioner keeps in such form as may be approved of by the Minister, with the consent of the Minister for Finance, all proper and usual accounts of all moneys received or expended by her and all such special accounts (if any) as the Minister, with the consent of the Minister for Finance, may direct.

Accounts kept in respect of each year are to be submitted by the Commissioner in the following year on a date (not later than a date specified by the Minister) to the Comptroller and Auditor General for audit and, as soon as possible after the audit, a copy of those accounts, or of such extracts from those accounts as the Minister may specify, together with the report of the Comptroller and Auditor General on the accounts, will be presented by the Commissioner to the Minister who shall cause copies of the documents presented to her to be laid before each House of the Oireachtas.

3.6 Reporting Requirements – Annual Report

In accordance with Appendix A of the ‘Business & Financial Reporting’ Annex to the *Code of Practice for the Governance of State Bodies*, the Annual Report should include:

- i. Noting that this Agreement has been reached with the Department of Justice and Equality and, in particular, indicating the DPCs level of compliance with the requirements of the Code of Practice for the Governance of State Bodies;
- ii. Confirmation that an appropriate assessment of the DPC’s principal risks has been conducted, including a description of these risks, where appropriate and associated mitigation measures or strategies.

3.7 Reporting Requirements – Financial Statements

In accordance with Appendix B of the 'Business & Financial Reporting' Annex to the *Code of Practice for the Governance of State Bodies*, the Financial Statements should include:

- i. Aggregate pay bill, total number of employees and compensation of key management level;
- ii. Total Costs incurred in relation to travel and subsistence and hospitality;
- iii. Details of expenditure on external consultancy/adviser fees;
- iv. Details of the number of employees whose total employee benefits for the reporting period fell within each band of €10,000 from €60,000 upwards;
- v. Details of termination/severance payments and agreements with a value in excess of €10,000, made within the period.

3.8 Protected Disclosures

In accordance with Section 21(1) of the Protected Disclosures Act 2014, the Data Protection Commissioner will establish and maintain appropriate Protected Disclosures Procedures for the making of protected disclosures by workers who are or were employed by the DPC and for dealing with such disclosures.

Procedures for dealing with disclosures from a person or entity who is/are external to the DPC should also be established.

3.9 Governance Obligations

As an independent statutory agency operating under the aegis of the Minister, the DPC is subject to a range of statutory and corporate governance obligations including the 2016 *Code of Practice for the Governance of State Bodies*. The DPC will ensure that all the necessary obligations, including those for risk management, internal audit and the Public Spending Code are fully complied with.

3.10 Compliance Statement to the Minister

To confirm compliance (or otherwise) with key provisions of the Code of Practice and the Governance Standard for Justice and Equality Sector Bodies, the Data Protection Commissioner will complete, on an annual basis, a Compliance Statement to the Minister in order to provide assurance to the Department that the systems of internal control, risk management and other areas of compliance are operating effectively. This report will address all of the relevant requirements of paragraph 1.9 of the *'Business & Financial Reporting Requirements'* Annex to the *Code of Practice for the Governance of State Bodies*.

3.11 Provision of Information to Members of the Oireachtas

In accordance with D/PER Circular25/2016 - *Protocol for the Provision of Information to Members of the Oireachtas by State Bodies under the aegis of Government Departments/Offices*, the DPC are obliged to:

- i. Provide and maintain a dedicated email address for Oireachtas members (oireachtasqueries@dataprotection.ie).
- ii. Put in place formal feedback processes to obtain feedback from Oireachtas members.
- iii. Comply with target deadlines and standards in terms of acknowledgements and responses to queries.
- iv. Designate a person at senior management level within the organisation with responsibility for ensuring the timely provision of information to members of the Oireachtas.
- v. Report annually (in the Compliance Statement to the Minister) on compliance with standards set out in Circular 25/2016.
- vi. Seek, where appropriate, to publish the response to queries from members of the Oireachtas on the DPC's website.

3.12 Governance obligations will also be reviewed as part of the overall monitoring process of this Agreement.

3.13 Comply or Explain

- i. In recognition of the DPC's particular circumstances and statutory independence, this Corporate Governance Assurance Document has been agreed between both Parties as satisfying the requirements of an Oversight Agreement as prescribed in the 2016 Code of Practice for the Governance of State Bodies. This Agreement sets out the broad corporate governance framework within which the office of the Data Protection Commissioner will operate and defines key roles and responsibilities which underpin the relationship between the Office and the Department of Justice and Equality.
- ii. In accordance with the Corporate Governance Framework for Justice and Equality Sector Bodies, it has been decided that since the DPC has a particularly high level of independence under EU law, the introduction of a detailed Performance Delivery Agreement would not be appropriate.

4. Relationship with Other Organisations

In addition to the DPC's regulatory functions laid down in the Data Protection Acts, various other statutes extend a supervisory role and/or consultation role to the DPC for the purposes of ensuring compliance with the Acts. Examples include the following:

4.1 Communications Regulator

The Data Protection Commissioner in conjunction with the Communications Regulator (Comreg) has responsibility for oversight of the additional data protection rules that apply to the activities of companies offering public communications services. These are laid down in Statutory Instrument 336 of 2011 which give effect to the European Union's Electronic Privacy Directive 2002/58/EC (as amended by Directive 2006/24/EC) and Directive 2009/136/EC.

4.2 Disability Act 2005

The Data Protection Commissioner also has responsibilities under the Disability Act 2005 (in relation to the processing of genetic data) and the British-Irish Agreement Act 1999 (in relation to North-South Bodies).

4.3 Customs

The Data Protection Commissioner is designated by section 6 of the Customs Act of 2001 as the national supervisory authority for the purposes of the Naples II Convention, continues to be so designated, and is designated as the national supervisory authority for the purposes of Article 24 of the CIS Decision.

4.4 Europol

The Data Protection Commissioner is designated as the national supervisory body for the purposes of the Europol Act 2012 and the Europol Council Decision 2009/371/JHA.

4.5 Eurodac

The Data Protection Commissioner is the supervisory authority in the state for the Eurodac system established under Council Regulation 2725/2000 (EU).

4.6 Internal Market Information System (IMI)

The Data Protection Commissioner is the supervisory authority in the state for the Internal Market Information System established under Council Regulation 1024/2012 (EU).

4.7 Criminal Justice (Forensic Evidence and DNA Database System) Act 2014

The Data Protection Commissioner has a role in relation to the inspection of random checks carried out by the Central Authority which checks the lawfulness of the supply of the data (sec135). A Deputy Commissioner of the DPC is a member of the DNA Database System Oversight Committee (Schedule 1, Sec1).

4.8 Communications (Retention of Data) Act 2011

The Data Protection Commissioner has a specified role under Section 4 of the Act in relation to the oversight of security measures to be taken by the service providers (Telco Companies) regarding retained data for the purposes of the Act.

5. Finance and Planning

5.1. Annual Budget

The annual budget for the Office of the Data Protection Commissioner is reflected as a separate subhead within the Justice and Equality Vote (Vote 24), for which the Secretary General is the Accounting Officer. ¹

The Office also has an allocation for receipts to be collected in respect of organisations required to register as data controllers and/or data processors under the Data Protection Act. Such receipts are transferred directly to the exchequer throughout the accounting year.

¹ The DPC budget will be reflected in subhead A.7 which is part of Programme A – *Leadership in and oversight of Justice and Equality policy and delivery*

5.2 Financial Shared Services

In common with other organisations in the Justice and Equality Vote, the Office avails of shared services for its payment and accounting processes. Invoice payments are processed through the central accounting system in the Department's Financial Shared Services Centre (FSS) in Killarney. Payroll and expense payments are processed by the Payroll Shared Service Centre (PSSC) which is under the remit of the Department of Public Expenditure and Reform (DPER). These payments are transferred to the general ledger in FSS via the same payroll interface files as other organisations attached to the Justice and Equality Vote.

5.3 Expenditure Limit

Expenditure and approval limits which apply across the Department and which are communicated by the Department's Financial Management Unit (FMU) also apply to the Office of the Data Protection Commissioner. Similarly, the requirements set out in Public Financial Procedures and the Public Spending Code also apply.

In the event of any "new" expenditure arising over €50,000 (excluding expenditure arising in the context of legal proceedings or expert data protection advisory services procured by the Commissioner in the performance of her statutory functions), the DPC will notify the Department's Financial Management Committee of the intention to place a contract for the purpose of providing assurance to the Committee that the proper procurement and public financial and spending procedures have been followed. Any such expenditure notifications are channelled through the FMU. Where DPER sanction is being sought, the request should be directed to Civil Governance Unit for onward transmission to DPER.

5.4 Additional Resource Requirements

Additional resource requirements are identified by the Office itself and are submitted as part of the estimates process. The estimates discussions are of a centralised nature and take place directly at senior official and Ministerial level with DPER at Vote Group level.²

In general, the overall budgetary provision for the Group is set for the current year and the two following years. Expenditure figures at vote and individual subhead level are reviewed, however, in advance of Budget Day in October. It is important that any additional requirements are identified well in advance of the Budget Day timescale so that they can be properly evaluated before forming part of the budgetary discussions in the July to October timeframe.

While expenditure for all subheads is monitored closely on a monthly basis, the budget holder should identify any deviations from budgetary profile as early as possible in the financial year so that any issues can be dealt with in the context of the overall budget for the Justice Vote Group well in advance of the end of the year.

5.5 Policy

The Data Protection Commissioner from time to time may liaise with the Data Protection legislative unit of the Department of Justice and Equality in terms of providing an independent view as concerns matters of data protection policy and matters pertaining to the statutory role of the Data Protection Commissioner.

²The Justice Vote Group currently comprises eight different Votes.

5.6 Audit

The legislation provides for the audit of the Office of the Data Protection Commissioner's accounts by the Comptroller and Auditor General.

5.7 Support Services

In addition to Financial Shared Services as outlined at 5.2 above, the Office of the Data Protection Commissioner avails of the shared services of the Department in relation to Human Resources.

The Data Protection Commissioner also has a Supplier Service Level Agreement with the Department of Justice & Equality IT Division for the provision of IT services and support to the office.

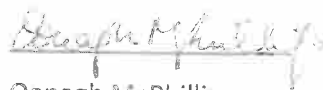
6. Duration and Signatories to the Agreement

It is hereby acknowledged that this document forms a key part of the governance and framework for the Office of the Data Protection Commissioner and will be updated as necessary, but at least every three years.



Helen Dixon
Data Protection Commissioner

Date: 12 March 2017



Oonagh McPhillips
Assistant Secretary
Department of Justice and Equality

Date: 15 March 2017