STATEMENT OF STRATEGY 2014-2016

Our Mission

To protect the individual's 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.

Our Mandate

The mandate of the Office of the Data Protection Commissioner is laid down in the Data Protection Acts 1988 and 2003. The Acts give effect to the European Union's Data Protection Directive 95/46/EC. The Directive lays down common minimum standards that apply across the European Economic Area.[1] It requires the establishment in each Member State of an independent authority to oversee implementation of the principles laid down in the Directive.

The Office shares with the Communications Regulator 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.

The Office 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).

The key principle underpinning data protection is that everybody 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. "Data controllers" - people or organisations

[1] The 28 Member States and Iceland, Norway and Liechtenstein

holding information about individuals must comply with the data protection rules in handling personal data, and individuals -"data subjects" -have corresponding rights.

The Data Protection Commissioner is responsible for upholding the rights of individuals, as set out in the Acts, and for enforcing the obligations upon data controllers. The Commissioner is appointed by Government and is independent in the exercise of his or her functions. The Commissioner makes an annual report to the Oireachtas. Individuals who feel their rights are being infringed can complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve it.

The Commissioner also maintains a register, available for public inspection, giving general details about the data handling practices of many important data controllers.

European Mandate

The Office also has responsibilities arising from Ireland's commitments at European level.

- Article 29 Working Party

The Commissioner is a member of the Working Party on data protection established under Article 29 of EU Data Protection Directive 95/46/EC. This Working Party brings together the Data Protection Commissioners of the EU, the European Data Protection Supervisor and the EU Commission. It discusses matters of common interest, and agrees common positions on the application of the Directive.

- European Databases and Data Protection Supervision
The Commissioner is designated under the Europol Act, 1997 as the "national supervisory body" for Ireland for the purposes of the Europol Convention. This function involves monitoring the activities of An Garda Síochána in liaising with Europol Headquarters in The Hague, The Netherlands. The Commissioner is a member of the Europol Joint Supervisory Body, which monitors Europol's operations to ensure that people's privacy rights are respected.

The Customs and Excise (Mutual Assistance) Act, 2001gave effect to the CIS Convention and the Customs Cooperation Convention in Irish law. The Data Protection Commissioner is designated under the Customs and Excise (Mutual Assistance) Act, 2001 as the "national supervisory body" for Ireland for the purpose of the Customs Information System Convention. This involves the monitoring of the activities of the Customs Service on its use of the Customs Information System (CIS). The Commissioner is a member of two European supervisory bodies in this regard: the CIS Joint Supervisory Authority and the CIS Supervision Coordination Group .

Since the coming into operation of the second generation Schengen Information System in 2013, the Schengen Joint Supervisory Authority has been replaced by the SIS II Supervision Coordination Group. The Commissioner is represented as an observer on this group pending Ireland's implementation of elements of the Schengen Information System. All of these initiatives involve the maintenance of large

databases with sensitive personal information, and therefore data protection safeguards are needed.

The Commissioner is also a member of the Joint Supervisory Body for Eurojust (co-operation by judicial and prosecution authorities).

Supervision structures at EU level for some of these initiatives may change over the lifetime of this Strategy Statement. New Regulations governing Europol and Eurojust are currently under discussion at EU level. These propose new supervision models with more direct supervision at central level by the European Data Protection Supervisor in coordination with national data protection authorities.

- *Eurodac*

The Commissioner is the supervisory authority in the state for the purposes of the Eurodac system established under Council Regulation 2725/2000. The recently adopted Eurodac Regulation and the additional responsibilities in relation to data protection will come into force during the lifetime of this Strategy Statement. Eurodac has been established as a means of Member States sharing fingerprint data in relation to asylum seekers. By sharing such data, it is intended that immigration authorities will be able to readily identify persons who have applied for asylum in another Member State or whose application has been rejected by another Member State. Eurodac is also subject to the overall supervision of the European Data Protection Supervisor, and the Commissioner is represented on the Eurodac Supervision Coordination Group.

International Mandate

Apart from his European role, the Commissioner is expected to contribute to, and cooperate with, data protection work carried out in various international fora and bilaterally. Notable among these are the International Conference of Data Protection and Privacy Commissioners, the OECD and joint enforcement initiatives such as GPEN (Global Privacy Enforcement Network).

This work is particularly important because of the presence in Ireland of many companies with international operations which involve the transfer of personal data on a global basis.

Analysis of our Environment

In pursuing our Mission, we must construct our strategy in line with the environment in which we operate. The constraints, challenges and opportunities we face are the key shapers of our Strategy.

Opportunities

-Adaptability and Commitment

We are a small, flexible and adaptable organisation. This enables us to identify new and emerging priorities for action at an early stage. The Office prides itself on having the capacity and the commitment to deal with any data protection issue that faces us, in a principled, pragmatic and effective way.

-European Framework
European Union law provides a common framework for data protection throughout the EU. The framework has been strengthened in the Lisbon Treaty, providing a specific legal basis for EU legislative action, a specific recognition of data protection as an independent human right and a specific obligation on each Member State to have an independent data protection authority[2]. The reinforced European framework provides strong underpinning for our activities and limits the extent to which domestic legislation can infringe on the individual's right to data privacy. This right is further reinforced by the domestic applicability of Article 8[3] of the European Convention on Human Rights and the related jurisprudence of the European Court of Human Rights, in accordance with the European Convention on Human Rights Act, 2003.

The EU Commission's proposal for a general data protection regulation, currently under discussion at EU level, is likely to place extra responsibilities on the Office. The Office will need to prepare adequately and ensure adequate resources to implement this reinforced regime during the lifetime of this Strategy Statement.

Challenges

-Economic and Budgetary Climate
The economic and budgetary situation over the coming three years is likely to remain very challenging, as effect is given to the National Recovery Plan 2011 to 2014 and beyond. This has already impacted on our Office in terms of budget cuts up to 2013. However, in 2013, the Office received extra resources, including specialist staffing, in recognition of its importance in regulating the many multinational companies located in Ireland which process data on a global basis.

However the economically difficult environment is still a challenge for the entire public sector and there is still a challenge in achieving policy outcomes that take full account of data protection considerations. There may be a tendency to view individual human rights, including data protection, as lesser priority, when the entire public sector is forced to deliver more with less.

The Office is fortunate to have secured support and recognition of its role in helping develop Ireland's digital economy. Pressures on this Office to deliver will increase as Ireland secures more multinational investment.

Technology
With continued progress, evolution and ubiquity in computerised technology, the risks of personal data disclosure, unauthorised processing or linkage increases for all. This is especially evident with Social Network technologies where personal data is a key ingredient of business models and is often available to a wide audience range.

It is incumbent on technology service providers to build protection of personal information into their systems from the very start, and to correct shortcomings where

[2] Article 16 of the Treaty on the Functioning of the European Union, Article 8 of the Charter of Fundamental Rights of the European Union
[3] Right to respect for private and family life

they exist. Adequate, appropriate and effective security measures also need to be addressed where personal information is sought, processed and retained.

At the same time, individuals right to privacy remain and must be defended, protected and upheld. We will continue to work to this aim while also promoting awareness of the risks and threats to personal data within the growing information society. For organizations and enterprise, we will promote the benefits of embracing the protection of personal information while also being compliant with law and regulation.

-The Individual and the State
The Government in the National Recovery Plan has reaffirmed the need to deliver more efficient and customer-focused public services, making maximum use of information technology. This approach will continue beyond the lifetime of the Plan. The government agenda includes sharing of personal data – including one-time-only collection of such data. The Government announced its intention in late 2013 to introduce a Data Sharing and Governance Bill. In the health area, where particular sensitivity attaches to data, a similar strategy is being pursued. In the area of crime detection and prevention, there is a growing tendency to use technology to collect and store information on large population groups.

Helping relevant State agencies to arrive at solutions which deliver the benefits of technology in a way that minimises the risk of loss of individual control over personal data and ensuring appropriate governance and audit remains a significant challenge.

-Changes in Data Protection Law
Indications are now that the new Regulatory environment at EU level may not be in place during the period of this Strategy Statement. However, in the intervening period, this Office intends to set an example at a practical level of how to best meet the data protection challenges posed by global investment, and to balance the needs of business and regulation.

Changes in our law recommended in the May 2010 Report of the Review Group on Data Protection[4], if implemented, would involve extra responsibilities for the Office, notably in relation to enforcement of data protection law.

-The International Dimension
Increasingly, personal data flows across national borders, often as part of internet-based networks. There is increasing tension between this reality and the operation of nationally-based data protection laws. As Ireland is host to many multinational companies, we must work towards solutions at European and international level that both facilitate international commerce and protect personal data.

High-Level Goals
In accordance with our legislative mandate:
1. To vindicate the individual's right to protection of personal data as laid down by law.

[4] Available at http://www.justice.ie/en/JELR/Pages/dprg_rpt_2010

2. To maximise levels of awareness and compliance with data protection obligations among those keeping personal data.
3. To provide timely, practical and easily understood advice to individuals and organisations.
4. 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.
5. To carry out our 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.
6. Prepare for a new Regulatory environment when new EU regulatory proposals in the area of data protection come into force.

Strategies

The following are the broad outlines of the approach we intend to adopt in carrying out the mandate assigned to us by law. Our annual Business Plans will break these down into Key Deliverables and Key Performance Indicators. Progress in achieving these strategies will be set out in our Annual Reports.

In 2014-2016 we will:

- Take proactive measures to improve levels of compliance with data protection obligations, using existing powers and any additional powers conferred by law

- Audit a wide range of organisations drawn from across the public, private and voluntary sectors with a view to assisting data controllers and data processors to achieve best practice in the area of data protection. Give priority to information-rich multinational companies providing services from Ireland to EU residents.

- Provide comprehensive, definitive and clear information and advice to our customers regarding data protection matters.

- Investigate complaints impartially and to the highest standards of customer service

- Contribute to strategies for the delivery of more effective, efficient and privacy-protective public services

- Improve levels of awareness among the public and those who process personal data about data protection rights and responsibilities, including through the effective enforcement of registration requirements.
- Contribute to the development of international data protection standards that facilitate international commerce while protecting personal data

- Work closely with other regulators to increase effectiveness, reduce regulatory burden and share best practices

- Work closely internationally to develop best practices and enforce data protection standards

- Develop the abilities, skills and competencies of staff to ensure continued improvement in organisational performance and enable staff to achieve their full potential.

- Perform our role and independent functions in a manner that is transparent, accountable and efficient, taking into account new obligations under proposed Freedom of Information Legislation and making maximum use of technology and shared services.

Performance Indicators

Awareness of data protection rights may be measured by periodic public surveys (budgets permitting).

Measurable standards of customer service (turnaround time for complaints, help-line response standards etc) are set out in our Customer Service Plan.

February 2014