ARTHUR COX

Data Protection Training

Colin Rooney, Partner, Technology and Innovation
Olivia Mullooly, Associate, Technology and Innovation

September 2015

Introduction

- Trinity College Dublin collects and uses personal data for a variety of purposes related to its core functions
- The College must comply with national and European privacy legislation
- Aim of this seminar:
  - assist staff dealing with personal data to do so in a way that complies with the College's legal obligations
  - upholding the personal rights of individual data subjects
  - provide staff across the College with an understanding of data protection laws as they apply to the College

What is the applicable law?

- The primary legislation governing data protection in Ireland is the Data Protection Acts 1988 and 2003 ("DPA")
- DPA fully in line with Data Protection Directive (95/46/EC).
- Additional legislation impinges upon specific areas
  - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011
    - lays down rules on type of consents required before direct marketing by phone, SMS, email, etc.
  - Irish courts have also held that a right to privacy exists under the Irish Constitution
  - Article 8 of the European Convention on Human Rights
    - provides each individual has a right to respect for his "*private and family life, his home and his correspondence*", subject to certain restrictions that are "*in accordance with law*" and "*necessary in a democratic society*"
    - European Convention on Human Rights Act 2003

Who is the regulator?

- DPA is enforced and administered by Data Protection Commissioner
- The Commissioner is responsible for:
  - upholding rights of individuals as set out in DPA
  - enforcing obligations upon data controllers & data processors
- The Commissioner
  - appointed by the government
  - independent in the exercise of his functions
- Individuals can complain to the Commissioner
  - staff will investigate the complaint
- Useful reference point: www.dataprivacy.ie.

When does the law apply?

- Some key concepts are critical to understanding the law
- Main rules are set out in 8 data protection principles in the DPA
- Principles (discussed below) apply to:
  - "**data controller**" - party who either alone or with others controls the contents and use of personal data
    - e.g. the College is a data controller in relation to staff and student data, therefore all College staff are responsible for the safekeeping of data
  - "**data processor**" - a party who processes personal data on behalf of a data controller
    - e.g. a payroll or website hosting provider
  - "**data subject**" – an individual who is the subject of the processed personal data
    - e.g. the College processes personal data relating to students, alumni, staff, visitors to the College, etc.

When does the law apply?

- DPA applies to data controllers *established* in Ireland that collect, store or process data about living people on any type of computer or in a structured filing system
  - Nationality of a data subject is not determinative
  - DPA does not apply to data kept by an individual for personal, family or household affairs, or for recreational purposes *only*
- The College *as a whole* is a data controller
  - DPA principles governs all of the various units in the College who control the use of personal data

What data are personal data?

- "**Personal data**" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.
  - Common examples include names, addresses, student numbers, photographs, staff numbers, mobile telephone numbers, dates of birth, etc.
  - The Commissioner adopts a broad view of what constitutes personal data
  - UK case law has provided a narrower definition of personal data (albeit criticised by the European Commission and resisted by the Commissioner)
- Factors to consider in determining if data is personal data include:
  - Is the data about the individual data subject?
  - Is the data subject the main or primary focus of the data?
  - Where does the data fall in a continuum of relevance or proximity to the data subject?
  - Is the data different in some respect because of the data subject's involvement?
- If in doubt as to whether data is personal data contact the **Information Compliance Officer**

Sensitive Personal Data

- Subset of personal data, being data relating to:
  - racial or ethnic origin
  - political opinions
  - religions or philosophical beliefs
  - trade union membership
  - physical or mental health
  - sexual life
  - the commission of offences or criminal convictions or proceedings
- Additional safeguards and a higher compliance burden apply
- Particularly relevant to the College Health Service, Counselling Service, Disability Service, certain data held by Tutors or other parts of the College who may receive health or conviction data in the course of performing their functions

Is paper/manual data covered?

- DPA applies to data held in computerised form or in paper form if it is part of a relevant filing system
  - "**manual data**" information that is recorded as part of a relevant filing system or with intention that it should form part of a relevant filing system
  - "**relevant filing system**" means any set of information relating to individuals to the extent that, although not processed by means of computer, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible
- Effectively structured paper files are covered by the DPA
- "**Automated data**" is data that is either being processed by means of equipment operating automatically in response to instructions given for that purpose or recorded with the intention that it should be processed by means of equipment operating automatically

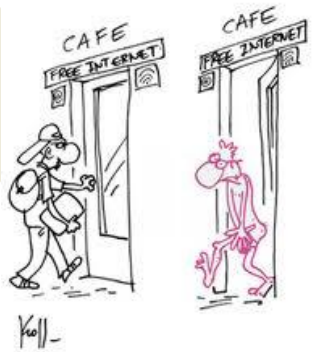
What is processing?

- The DPA only applies to the "processing" of "personal data"
- Processing is extremely widely defined
- Difficult to imagine any use of personal data which would not amount to processing for the purposes of the DPA
- Effectively processing covers all forms of data use (whether active or passive)

What are the basic rules?

- Certain core data protection principles govern all processing of personal data by a data controller
- Personal data must:
  - be obtained and processed fairly
  - be kept for only one or more specified, explicit and lawful purposes
  - not be used or disclosed in any manner incompatible with these purposes
  - be kept safe and secure
  - be accurate and where necessary kept up-to-date
  - be adequate, relevant and not excessive in relation to the purposes
  - not be retained for longer than is necessary for the purposes
- Also a copy of the personal data relating to an individual must be given to that individual on written request (subject to limited exceptions)
- All data controllers (whether or not required to register with the Commissioner) are required to observe the principles
- Data processors are required to comply with the **security principle**.

What is “fair” obtaining?



- “Fair Obtaining” is most important of data protection rules
- Requires *transparency* and *full disclosure* of all proposed uses at data capture
- Certain obvious uses may be implied by circumstances of data capture
- To obtain personal data fairly, the DPA requires that the data subject “*is provided with, or has made readily available to him or her*” at the time of processing the data, at least the following information:
  - the identity of the data controller (often implied)
  - the purpose behind the data collection
  - the persons or categories of persons to whom the data may be disclosed
  - any other information which is necessary having regard to the specific circumstances
  - the categories of data concerned
- Otherwise any personal data collected from the data subject will not have been collected fairly and the data controller will have infringed the DPA
- Very important that the College identifies all points of data capture where it seeks personal data so as to ensure that appropriate privacy notices, consents, etc. are obtained and recorded
  - If secondary uses are anticipated specific consents may be necessary

What is “fair” processing?

- Other core data protection principle = processing of data must be fair
- Usually requires
  - consent for particular data use ***or***
  - that the processing is otherwise required for a College obligation
- Example of unfair processing might include:
  - emailing a student class list to a researcher to assist in a research project on student behaviours (assuming data is not “anonymised”)
  - disclosing a student’s examination results to a person not specifically authorised by the student to receive them

Is consent required?

"Sign here to indicate you have no idea what you've signed."

- In general where consent to processing has been obtained from the data subject, processing will be permissible
- Pursuant to Section 2A of the DPA, consent is not required where the processing is necessary for certain purposes, including:
  - for the performance of a contract to which the data subject is a party
  - for compliance with contractual legal obligation
  - where the processing is necessary for a public purpose
  - for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed *except* where the processing is unwarranted by reason of prejudice to the fundamental rights of the data subject
- If above criteria do not apply, consent will usually be necessary

Processing sensitive personal data

- If processing sensitive personal data, consent cannot be implied and must be "**explicitly given**".
- Without explicit consent, other pre-conditions for the lawful processing of sensitive personal data include where the processing is necessary for:
  - compliance with employment law obligations
  - protecting the vital interests of the data subject
  - processing by a not-for-profit organisation
    - political, philosophical, religious or trade union purposes only
  - obtaining of legal advice and establishing or defending of legal rights
  - public functions (administration of justice, etc.)
  - medical purposes.
- Sensitive personal data should be restricted to those members of staff that
  - specifically require such access to carry out their functions
  - who have received appropriate training

What is the age of consent?

- DPA does not provide any specific minimum age for giving consent to data processing
- Data controllers must decide if a minor (anyone under the age of 18) is capable of appreciating the implications of giving consent
- If unable to appreciate the nature and effect of consent (due to physical or mental disability or age), consent should be given by a parent, guardian or relative
- The College generally considers all students to be capable of appreciating the implications of giving consent

Sharing personal data

- Disclosure of personal data outside of the organisation must be legitimised by:
  - one of the processing justifications under Section 2A of the DPA
  - if the disclosed data is sensitive personal data, one of the Section 2B justifications
- In addition, Section 8 of the DPA exempts certain narrow categories of processing from the restrictions that would otherwise apply, e.g.
  - processing required to investigate offences
  - urgent processing required to prevent injury or damage to property
  - processing required by rule of law, etc.
- Where the Section 8 exceptions, the College is permitted to process personal data without necessarily addressing the data protection rules that would normally apply e.g. informing the data subject about the proposed use of the data or seeking consent from the data subject.
- Hence DPA will not prevent disclosure of information where the College is legally obliged to make the disclosure
  - e.g. staff salary details must be provided to the Revenue Commissioners

Sharing personal data (cont.)

- Important to exercise caution when disclosing personal data, notably if disclosure is in response to request from a third party
- Prudent checks include:
  - Requester should be asked to make their request in writing
  - identity of the requesting individual should be verified
- Ordinarily the College will not disclose personal data to parents, guardians or other representatives of a student without the student's consent
  - BUT, in exceptional circumstances, e.g. in the case of potential danger to the health or well-being of a student or if a representative such as a solicitor or politician has written to the College making it clear that they are acting on behalf of the student
- Sometimes the College enters into contracts that require the transfer of student data, e.g. exchange agreements
  - Such contracts are managed by the Secretary's Office and will contain specific provisions governing the sharing of personal data

Security obligations

- Section 2C of the DPA requires that "*appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data*"
- In determining what an appropriate security measure is, the data controller must:
  - take into account technological development
  - cost of implementing the measures
  - ensure that the measures provide a level of security appropriate to nature of data and harm that might result from unlawful processing
- Appropriate technical security arrangements depend on nature of the data and the context of processing
  - include password protection, data encryption, virus prevention, firewalls, fireproof filing cabinets, etc.
- Important to train staff in both data protection law and data handling policies
- Security issues must be carefully considered when personal data are being destroyed or being transferred outside of College (notably if over a network)
- Further guidance can be found in the extensive IT security policies of the College (http://www.tcd.ie/ITSecurity/policies/) or by contacting the IT Security Officer (in relation to IT security) or College Security (in relation to physical security)

Obligation to Report a Breach?

- Despite **Personal Data Security Breach Code of Practice** presently no explicit obligation to notify Commissioner's Office or data subject if breach of information security.
- Exception: ISPs and Telecos.
- However may be advisable to do so.
- First consult with **Information Compliance Officer**
- **Note**: this position will change shortly on foot of EU law

Engaging data processors

- Where the College engages a third party to process personal data on its behalf, it is a legal requirement that the College has in place a ***contract in writing,*** pursuant to which College must ensure that:
  - the processing by the data processor is undertaken only in accordance with College's instructions
  - the processing by the data processor is undertaken only for the purposes, and in the manner, stated in the agreement
  - its staff are adequately trained in data security measures
  - there is a contractual obligation on the data processor to implement and maintain specific security measures, both in terms of physical security and technological security
  - the College has rights of access to and inspection of the processor's premises and systems to ensure security measures are being implemented
  - it can control the data processor's ability to sub-contract any of its obligations to third parties
- Agreements to engage third party service providers to process personal data are managed by the **Secretary's Office**

Seeking access to personal data

- Data subjects have certain rights conferred under the DPA
- Most significant right being right to obtain a copy of personal data
- Within 40 days of a data subject access request (subject to data subject paying(maximum) fee of €6.35), a data controller must:
  - confirm whether the data kept includes data relating to the data subject
  - supply data subject with a copy of such data in intelligible form
    - (subject to a "disproportionate effort" exemption)
  - inform data subject of the purpose(s) for the processing of his/her data
  - notify data subject of the identity of those to whom the data controller discloses the data
  - inform data subject of the source of the data, unless it is contrary to public interest
  - explain the logic involved in automated decisions
- Right of access is extremely wide-ranging
- Unless a relevant exemption applies, data subject is generally entitled to see their personal data contained in all locations

Seeking access to personal data

- Data subject is entitled to see only his/her own personal data, not any information which relates to anyone else or more general records
  - but note College's Freedom of Information obligations
- Very limited grounds for refusing a data subject access request
  - no carve out for defamatory statements, harmful content or commercially sensitive information.
- The Commissioner tends to the view that a broad interpretation of personal data should apply
- Highly significant decision of the English Court of Appeal, Durant v Financial Services Authority in 2004
  - Dramatically restricted the scope of data protection legislation in England and Wales
  - To be part of a data subject access request data must "relate to" the individual
  - Is information biographical in a significant sense and focused on the individual?
- To ensure a coordinated and appropriate response to data access requests, requests should be directed to the College's Information Compliance Officer

Requests for health data

- Request for health data may be refused if disclosure is likely to seriously damage the physical or mental health of data subject
  - **Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989)**
- Data controllers (if they are not health professionals) must consult with the individual's doctor before disclosing health data.
- Similar exemptions in respect of access to social work data
  - **Data Protection (Access Modification) (Social Work) Regulations, 1989 (S.I. No. 83 of 1989)**
- Disclosure can be refused if it is likely to cause serious damage to the physical or mental health or emotional condition of data subject
- Of specific relevance to data processed by the College or its service providers in the context of student or staff counselling services

Examinations data

- Examinations data which identifies any particular student is "personal data"
- Publish examinations data as anonymously as possible
  - e.g. student numbers instead of names
- Right of access to examination data is specifically dealt with by DPA
- Right for students to access their scripts and discuss their performance is outlined in **General Regulations and Information Section of the College Calendar**
- Students should contact the relevant Director of Undergraduate Teaching and Learning or Course Coordinator
- Note if accommodation has been offered to a student who may suffer from a disability, this "sensitive personal data" should not be shared with any parties within the College unless they have a *need to know*

Automated decisions

- Right to prevent the data controller from taking evaluation decisions, that would '*significantly affect*' data subject, by automated means alone
- If personal data are being processed automatically for the purpose of evaluating matters relating to data subject and processing is sole basis of a decision significantly affecting the data subject, data subject is entitled to be informed by the data controller of the logic behind the decision taking
- No obligation to disclose a trade secret

Rectification and erasure

- Right to have data that is held in contravention of the data protection principles rectified or erased within 40 days of request being made
- Data controller must also notify
  - individual making the request and
  - any person to whom the data was disclosed during the 12 month period prior to the request
  - unless this involves disproportionate effort

Duty of care

- Section 7 of DPA
- Data controllers & data processors owe duty of care to the data subject in relation to processing of personal data
- Injury suffered by a data subject may include damage to reputation, financial loss or mental distress
- Data subject can bring a civil action in the Irish courts
- To date such claims have been rare
- Duty of care is in addition to right of Commissioner to investigate complaints made by data subjects

Transferring personal data

- Prohibition on transfer of personal data to a country outside the European Economic Area ("EEA") unless such country ensures an "*adequate level of data protection*"
- Does not apply to transfers of personal data to certain "**safe countries**" (e.g. Argentina, Canada, Switzerland, Guernsey, The Isle of Man, Jersey, Faroe Islands, etc.)
- Otherwise special conditions must be met before transferring personal data outside the EEA
- Transfers are ordinarily managed using:
  - data subject consent
  - European Commission approved 'model form clauses'
  - 'Safe Harbor' scheme (for data exports to the US)
  - (less frequently) binding corporate rules

Sending Data Abroad (cont.)

Safe Countries

Argentina
Canada*
Switzerland
Guernsey
The Isle of Man
Jersey
Faroe Islands
Israel
New Zealand
Uruguay

*restrictions apply

Types of transfers approved by the Commissioner

‘Safe Harbor’
Binding Corporate Rules
Model Contracts

Transferring Personal Data

- Cross border transfers of data can also be legitimised where the transfer:
  - is required by law
  - takes place with the data subject's consent to the transfer
  - is necessary for the performance of a contract to which the data subject is party
  - is necessary for the taking of steps at the request of the data subject with a view to entering a contract with the data controller
  - is necessary to conclude or perform a contract between the data controller and someone other than the data subject in cases where the contract is entered into at the request of the data subject or where the contract is in the interests of the data subject
  - is necessary for reasons of substantial public interest
  - is necessary for obtaining legal advice or for legal proceedings
  - is necessary to: prevent injury or other damage to the data subject's health; prevent serious damage to his property; or protect his vital interests in some other way
  - is authorised by the Office of the DPC
- No units of the College should transfer any data outside the EU without first contacting the Secretary's Office and IS Services
- This includes the uploading personal data to a cloud server which is based outside the EU (see further TCD Cloud Computing Policy)

Powers of the Commissioner

- The Commissioner has the power to:
  - carry out investigations to ensure compliance with the DPA
  - obtain information and issue enforcement notices (in respect of contraventions which are not criminal offences in themselves)
    - can require persons or legal entities to take steps that may include ceasing data capture
    - failure to comply with an enforcement or other notice constitutes an offence
  - prepare and publish codes of good practice in particular areas
  - bring prosecutions and ask the courts to impose criminal fines on data controllers / processors (or directors / managers)
- Offenders (under DPA) are liable on summary conviction to a fine not exceeding €3,000 and on indictment, not exceeding €100,000
- Court may also order the forfeiture, destruction or erasure of data connected with the offence
- Enforcement action by the Commissioner may lead to negative publicity for the College

Registration obligations

- All data controllers must comply with the data protection principles
- Not all data controllers are required to register with the Commissioner's office
- Certain special organisations must register, including
  - government bodies / public authorities
  - persons whose business consists wholly or mainly in direct marketing
  - anyone processing personal data related to mental or physical health (e.g. health professionals
  - anyone processing genetic data, etc.
- It is an offence to process personal data without an appropriate entry on the register of data controllers, unless an appropriate exemption exists.
- Currently certain parts of the College are already registered with the Commissioner, e.g.
  - Centre for High Performance Computing and
  - TILDA (Irish Longitudinal Ageing) Study
- All registrations and renewals should be coordinated through College's **Information Compliance Officer**

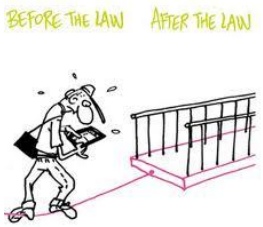
Retention of personal data

- Personal data should not be kept for longer than necessary for the purpose for which it was acquired
- No specific retention periods are set by the DPA
  - consider for how long data needs to be kept
  - set specific retention periods (e.g., under applicable employment law, tax law, the Statute of Limitations, etc.).
- Adhere to obligatory retention periods set by external professional regulators

Data Protection Officer

- Not strictly necessary
- However College has appointed an Information Compliance Officer
- The Information Compliance Office, which sits within the College Secretary's Office, is the primary office responsible for compliance with Data Protection Law within the College
- The Information Compliance Officer is Sinead MacBride, College Solicitor
- Useful for each area to nominate a Data Protection Liaison Person to link in with the Information Compliance Officer

Reform of data protection law



- The European Commission, the European Parliament & European Council discussing proposals for overhaul of data protection rules in EU
- Rationale is to reform the law so that a unified data protection regime will exist across EU
- If proposal adopted:
  - increased compliance obligations of data controllers
  - possibility for fines of up to 5% of global turnover
- Expected that new law will be enacted by Regulation
- Timing of changes is unclear (possibly effective in 2016/2017)

Further Information

- Range of published College policies which are available at www.tcd.ie/policies. For example
  - Data Protection Policy
  - Child Protection Policy
  - CCTV Policy
  - IT and Network Code of Conduct
  - IT Security Policy
  - Mental Health Policy
  - Records Management Policy (which is currently subject to review)

ARTHUR COX

Questions?

September 2015