CSCU9B3
Database Principles and Applications

Database administration

Legal and Professional Issues (GDPR, DPA, FOI)

Database Administration

Ritchie: Chapter 4

Databases vary in size from single use to thousands of users.

Here we consider some over-arching concerns and special technical roles

- Data Dictionary
- Data Administrator
- Database Administrator

- And then look at professional and legal issues around data handling

The Data Dictionary - I

- A DBMS must provide facilities to allow users to find out the properties of the stored items (**metadata**).
- These facilities may also be used by components of the DBMS itself.
- Collectively, these facilities are called the **Data Dictionary** (or the **System Catalogue**).
- The Data Dictionary must hold information about the tables, views, forms, queries, and reports stored in the database.
  - for example, it stores information about the name, types, sizes, and constraints that apply to each of the tables in the database
- It must also store information about the users of the system.
  - For example, it stores the names and details of authorised users including information about which areas of the database are accessible to each user
- Some of this information is accessible only to the DBA.

The Data Dictionary - II

- In a relational DBMS, the Data Dictionary is often made to look as if it were made up of tables.
- These tables are views.
- For example, in Oracle there are many tables with names such as **USER_xxx** which give information relating to a particular user.
  - For instance, the table **USER_CATALOG** shows all tables and views owned by the current user. (A synonym for this is **CAT**)
  - This table has only two columns: name and type
- In MySQL INFORMATION_SCHEMA provide access to metadata.

The Database Administrator - I

- Within any organisation using a shared DBMS, we will expect to find a **Database Administrator** (**DBA**).
- At the very minimum (where the users use the DBMS for their own independent purposes), the DBA will be responsible for the orderly running of the program.
- For instance, an “instance” of ORACLE or MySQL runs all the time (even when there are no users logged on to it)
  - and users’ data is not stored in separate files, but in common data areas…
  - and is backed up and journalled (logged) together…
  - so at the very least there must be someone who makes sure that all this happens properly.

The Database Administrator - II

- However, in most organisations (perhaps in all organisations of any significant size), many users will be sharing data
  - and the shared data will be crucial to the core business
- The data may be divided into different systems - for example the University has
  - Finance
  - Student Records
  - Recruitment and Admissions
  - Vacation letting
  - Estates and Buildings
  - Payroll
  - Personnel
- Under these circumstances the managerial role of the IS professional is very important indeed (and there will be a team)

The DA and the DBA - I

- There is often a distinction between the roles of the **Database Administrator** and the **Data Administrator**, both of which have specific responsibilities that complement each other.
  - The DA has a more strategic and managerial role.
  - The DBA has a more technical role.
- The DA will be responsible for the Information Strategy of the organisation as a whole (i.e. transcending the various subsystems)
- and will be concerned with large-scale developments (e.g. moving subsystems between platforms, developing new subsystems, ensuring resilience, developing & maintaining standards, policies & procedures etc.)

The DA and the DBA - II

- The DBA role is concerned more with managing a particular (sub)system on a particular platform
- The DBA will have roles both during the setting-up of a system, and, later, while it is running.
- The DBA will
  - with the DA, participate in deciding the information content of the database
  - write the conceptual specification (“conceptual schema”)
  - decide how the data should be stored: use the facilities of the DBMS to provide the mapping from the logical to the physical

The DA and the DBA - III

- The DBA will also
  - write “sub-schemas” for user views
  - document the views
  - allocate ownership rights and duties
  - with the DA, adjudicate between different interests
  - use the DBMS management tools to monitor, tune, reorganise, protect, backup, and reload

Management tools used by the DBA

- Any mature DBMS will provide tools to:
  - bulk load data from files in other formats
  - restructure data: for example to distribute data across several sites
  - provide differential access to data in ways that can be configured and restructured
  - maintain dynamic backup and restore facilities to enable rapid recovery of a DBMS whose platform crashes
  - (these facilities may be automatic but configurable by the DBA)
  - give access to data about the DBMS, its contents, its users and its performance (via the Data Dictionary)
  - retune parameters to improve performance

Data Protection Legislation

- Clearly, the roles of DA and DBA have specific duties related to the data handling (legal, professional, security)
- As an individual you should know about your rights with respect to data held about you
- As an information professional you may have to deal with other people's information, and you may have to advise others on the law
- The current legislation is the **General Data Protection Regulation 2018**, and the **Data Protection Act 2018** which is substantially different from the earlier legislation (Data Protection Acts 1998, 1984)
- The Freedom of Information Act 2000 (UK) and Freedom of Information Act 2002 (Scotland) may also have impact if you work for a public authorities

- https://ico.org.uk/

GDPR legislation - definitions

- First, some points about the words
  - *Data* is not just computer data. Any systematic collection of records is covered, including paper records (part of a filing system)
  - *Personal data* is information that relates to an identified or identifiable individual, e.g. with a name, number, IP address, cookie.
  - Personal data must "relate to" an individual: it must concern them (consider the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual)
  - *Sensitive personal data* includes racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
  - A *data subject* (a natural person) is any living individual who is the subject of personal data

GDPR legislation - definitions

- A *controller* determines the purposes and means of processing personal data.
- A *processor* is responsible for processing personal data on behalf of a controller.
- "*processing*" means collected, held, obtained, organised, adapted, retrieved, consulted, disclosed, transmitted, deleted …
- … whether or not by automated means
- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

Seven principles

- Seven key principles at the heart of processing data:
  1. Lawfulness, fairness and transparency
  2. Purpose limitation
  3. Data minimisation
  4. Accuracy
  5. Storage limitation
  6. Integrity and confidentiality (security)
  7. Accountability

Lawful basis for processing - I

You must have a lawful basis in order to process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Lawful basis for processing - II

- GDPR requires controllers to be more careful about the purposes of processing and the lawful basis for processing
- Special category data: needs additional conditions for processing this data (see sensitive personal data)
- Criminal offence data: needs additional legal authority for processing this data

- https://www.stir.ac.uk/about/faculties-and-services/policy-and-planning/legal-compliance/data-protectiongdpr/privacy-notices/staff/
- https://www.stir.ac.uk/about/faculties-and-services/policy-and-planning/legal-compliance/data-protectiongdpr/privacy-notices/students/

Schedule 3 (Sensitive personal data)

At least one of:

- Subject has given **explicit** consent
- Legally necessary for employment
- When consent cannot reasonably be obtained, to protect vital interests of anyone
- When consent unreasonably withheld, to protect the vital interests of third parties
- As part of membership of non-profit groups for “political, philosophical, religious or trade-union purposes”
- Already made public by subject
- Necessary for legal or medical processes
- Monitoring of equal opportunity of racial/ethnic groups

The Eight Subject rights

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Security

- Data controllers must ensure that they process personal data securely by means of ‘appropriate technical and organisational measures’
- Doing this requires consideration of things like risk analysis, organisational policies, and physical and technical measures.
  - Consider state of the art and costs of implementation
  - Appropriate to your circumstances and processing risk
- For example,
  - use pseudonymisation and encryption.
  - ensure access and availability to personal data can be restored in a timely manner in the event of a physical or technical incident
  - ensure appropriate processes are in place to test the effectiveness of measures
  - undertake any required improvements.

Data Controllers

- Not everyone who holds data is a data controller (Not covered: domestic purposes, law enforcement, national security)
- There are also exemptions (e.g. public protection, journalism, parliamentary privilege, social work, confidential references, exam scripts and marks)
- Data controllers must be **responsible** for compliance with the GDPR and **demonstrate** compliance. This means
  - being proactive and organised about data protection
  - being able to evidence the steps taken to comply
  - pay a data protection fee (£40 - £60 - £2900) depending on the size of the organization
  - appoint a data protection officer (public bodies, and certain types of processing)
  - should ensure there is robust breach detection, investigation and internal reporting procedures in place.

Data Breaches and Offences

- Data breaches must be reported
  - to the relevant supervisory authority within 72 hours of becoming aware of the breach
  - to individuals, if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms
- Offences include
  - Data breaches
  - Processing in a non-compliant way
  - Infringement of an individual's privacy rights
- The commissioner issues enforcement notices and applies fines
  - Up to €10 million, or 2% annual global turnover – whichever is higher.
  - Up to €20 million, or 4% annual global turnover – whichever is higher.
- Individuals may seek compensation for damage

Some questions

- Does the University need to get each student's explicit consent to every detail of their information handling?
- What happens if a student's parent rings up to enquire about the student's progress?
- May results be posted on noticeboards? On the WWW? May graded work be returned using a communal pigeonhole?
- Can a student, making a Subject Access Request
  - see their own exam scripts?
  - ask about how their degree was classified? Request that the classification is reviewed by a human?
  - ask to see every internal email that mentions them?
  - ask to see every paper document referring to them?

Overview of Freedom of Information (Act)

- The public's 'right to know'
- Applies to all information
- Proactive disclosure via a Publication Scheme
- Responding to individual enquiries
- Based on good records management
- The Freedom of Information Act enables people access to information which is held by/on behalf of public authorities and those bodies carrying out a public function, and which does not fall under the access regime of personal information.

Your information rights

- The Freedom of Information Act facilitates access to information held by public authorities in two ways:
- * By requiring public authorities to adopt and maintain publication schemes, which should have the effect of improving the amount and quality of information routinely made available to the public.
- * By creating a right to make a request for information (effective from 1 January 2005). Anyone, including people living abroad, non-UK citizens, journalists, political parties, lobby groups and commercial organisations, will have the right to ask public authorities for any information they hold.

- More about the (Scottish) act can be found at:
- http://www.itspublicknowledge.info/

Under the Freedom of Information (Scotland) Act you have the right to get information from any of the following Scottish public authorities or office-holders:

- Scottish Ministers in charge of all departments of the Scottish Executive and its agencies.
- The Scottish Parliament.
- Non-ministerial office holders in the Scottish Administration, including the chief medical and dental officers; the chief inspectors of constabulary, prisons, fire services and school;, rent officers; social work inspectors.
- Local government, including councils, assessors, fire services, licensing boards and the Strathclyde Passenger Transport Authority.
- The National Health Service, which includes NHS boards, community health partnerships, hospitals, GPs, dentists, pharmacists, opticians and other health professionals.
- Educational institutions such as universities and colleges.
- The police.
- Other public authorities, including more than 50 types of Scottish public authority not covered in the categories above. They range from the Scottish Arts Council to the Water Industry Commissioner for Scotland.
- Companies that are wholly owned by one or more public authorities.

What kind of information do I have a right to see?

- You can ask to see any kind of recorded information from a Scottish public authority, however old the information is. That includes information recorded on:
  - paper
  - computer files, including e-mails
  - video
  - microfiche

Examples of information you can find out

- The number of complaints made about a particular service, for example street cleaning or refuse collection and whether action was taken as a result.
- Information showing whether public authority policies are working well – for instance, is a Community Policing Initiative reducing crime in the local area?
- Information that would reveal whether a contract is providing value for money, for instance, what standards have been agreed with agencies contracted to supply hospital cleaning or catering services.
- Why decisions affecting local services were made, such as a decision to cut back some services at your local hospital, or to combine local primary schools.
- How public authorities decide who gets priority on waiting lists for services such as health or housing.

Information You Cannot Find Using FoI

- Whether or not somebody has a criminal conviction
- Who has borrowed that library book that you want
  - Information like this about individuals is protected by DPA/GDPR
- How many plastic bottles are collected by the recycling team
  - This information is not kept – you cannot ask for research to be done!
  - There is also a limit on how difficult it needs to be to collate information, even it is stored
- How much money my University spin-out company makes from selling electronic data acquisition boards each year
  - Although the company is fully owned by the University, I can argue that the information is commercially sensitive and not have to disclose it
- What products Apple is currently developing
  - You cannot use FoI to ask private (non-government) organisations anything
- Secret military or security related information

End of Lecture

Would you like to ask anything?

Don’t forget to read the notes again.

Carefully read the ICO guidance on GDPR and FOI

Look out for new stories on these issues