



UCEM Institutional Research Repository

Title	APC Workshop slides on ethics and professional standards, business planning, data management, accounting principles and procedures, conflict avoidance, conflict management and dispute resolution, RICS Rules of Conduct, sustainability.
Author(s)	David Hourihan, David Hourihan, David Hourihan and David Hourihan
ORCID	https://orcid.org/0000-0003-1405-3130 ; https://orcid.org/0000-0003-1405-3130 ; https://orcid.org/0000-0003-1405-3130 ; https://orcid.org/0000-0003-1405-3130
Type	Conference or Workshop Item
Publication title	
Publisher	
ISSN/ ISBN	
Publication Date	14 January 2020
Version	
DOI	
Repository link	https://ube.repository.guildhe.ac.uk/id/eprint/206/
Link to publication	

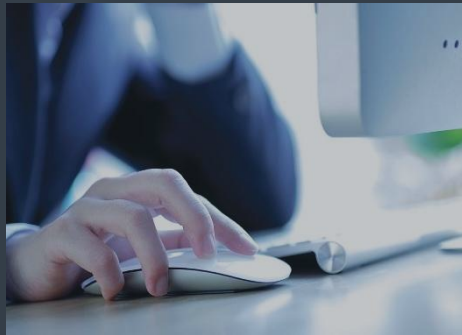
Copyright:

UCEM aims to make research outputs available to a broader audience via its digital [Repository](#). Where copyright permits, full text material held in the Repository is made freely available. URLs from GuildHE Research Repositories may be freely distributed and linked to. Please refer to each manuscript for any further copyright restrictions.

Reuse:

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page, and the content is not changed in any way.

DATA MANAGEMENT



Data Management



Summary Profile



Module Leader:

David Hourihan

MSc Pro Invest FSCSI FRICS FHEA

Industry

- Chartered Surveyor and specialist in office agency, retail asset management and valuation.
- 17 years of commercial real estate experience across the UK and Ireland.
- Previous positions with international firms including JLL and Colliers International.
- Acquisition and asset management instructions for clients including Société Générale, Metzler Bank, Mobil Oil, Scottish Widows, Aviva and British Land.

Research

- Member of the Investment Property Forum (IPF) Research Steering Group.

Academia

- Completed MSc in Property Investment at UCEM in 2008.
- Programme Leader for the MSc Real Estate.
- Module Leader for 'Real Estate Investment' module on the MSc RE and BSc REM programmes.

APC

- **APC Chairman for the RICS.**

Data Management

By the end of the programme the learners will be able to:

- Know about GDPR.
- Have knowledge and understanding of the sources of information and data.
- Be able to identify information and data systems applicable to their area of practice.
- Identify methodologies and techniques most appropriate to collect, collate and store data in relation to their area of practice.

Data Management

Contents:

1. APC Notes.
2. GDPR.

Knowledge and Understanding of the sources of information and data.

Identify information and data systems applicable to your area of practice.

Identify methodologies and techniques most appropriate to collect and store data in relation to your area of practice.

Data Management - APC Notes

Final Interview

- Level 1 only.
- At most one question will be asked.
- Currently (because it is a “hot topic”) a question on GDPR is more likely to be asked than any other question.
- By the time you take your APC will it still be a “hot topic”?

Data Management - APC Notes

RICS APC Requirements - Level 1

“Demonstrate knowledge and understanding of the sources of information and data, and the systems applicable to your area of practice, including the methodologies and techniques most appropriate to collect, collate and store data.”

Examples of knowledge comprised within this level are:

- The use of published sources of data, particularly BCIS.
- How data is collected, analysed and stored within your employer's organization.
- How project information is stored within your employer's organization.
- How electronic database systems work.
- The use of computerised central project databases or Building Information Modelling, the benefits, challenges and dangers.
- How technical libraries are set up and used.
- **Legislation applicable to data management and data access – (GDPR),**

Data Management - GDPR

The EU **General Data Protection Regulation** (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organisations across the region approach data privacy.

Like its predecessor, the **GDPR** is designed to protect personally identifiable information (**personal data**).

What constitutes personal data? Any information related to a natural person or '**Data Subject**', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address. The legislation applies not only to electronic data but any records that are stored in a form that is easily searchable.

Data Management - GDPR

Key Terms (Remember):

Data Subject – the person whose personal data it is, ie you and me.

Data Protection Authority (DPA) – the national authority responsible for implementing and enforcing GDPR. In the UK it is the ICO (Information Commissioners office).

Data Protection Officer – the individual person within an organisation responsible for data protection compliance.

Data Controller - This is a person who decides the purpose for which any personal data is to be processed and the way in which it is to be processed.

Data Processor - third parties that process data on behalf of the Data Controller and includes IT service providers

Data Management - GDPR

Does my business need to appoint a Data Protection Officer (DPO)?

- DPOs must be appointed in the case of:
 - a) public authorities,
 - b) organizations that engage in large scale systematic monitoring,
or
 - c) organizations that engage in large scale processing of sensitive personal data (Art. 37).
- If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO.

Data Management - GDPR

What is the difference between **a data processor** and **a data controller**?

A **controller** is the entity that determines the purposes, conditions and means of the processing of personal data, while the **processor** is an entity which processes personal data on behalf of the controller.

Data Management - GDPR

What about Data Subjects under the age of 16?

Parental consent will be required to process the personal data of children under the age of 16 for online services; member states may legislate for a lower age of consent but this will not be below the age of 13.

Data Management - GDPR

Key changes

1. **Increased Territorial Scope** - GDPR now applies to all companies processing the personal data of **data subjects** residing in the European Union, regardless of the company's location.
2. Private individuals not engaged in business activities are now exempt. You're free, at home, to store personal contact details - providing, of course, this is for personal use only.
3. **Penalties** - Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).
4. **Consent** - Companies will no longer be able to use long illegible terms and conditions full of legalese. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Data Management - GDPR

Key changes

5. **Breach Notification- mandatory** where a data breach is likely to “result in a risk for the rights and freedoms of individuals”. This notification must be done within 72 hours of first having become aware of the breach. **Data processors** will also be required to notify their customers, the controllers, “without undue delay” after first becoming aware of a data breach.
6. **Right to Access** - Individuals will now have the right to obtain confirmation that their data is being processed and access to their personal data.

Data Management - GDPR

Key Changes

Right to be Forgotten - Individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'.

Individuals have the right to have their personal data erased if:

1. the personal data is no longer necessary for the purpose to which it was collected/processed;
2. you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
3. you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
4. you are processing the personal data for direct marketing purposes and the individual objects to that processing;
5. you have processed the personal data unlawfully;
6. you have to do it to comply with a legal obligation.

Data Management - GDPR

How will GDPR affect surveying practices?

For a chartered surveying firm, here are just a few of the types of data that will be covered by GPDR:

1. Data you hold to service your clients, for example: Data in your valuation systems; Data in your compliance systems, including accounts, bookkeeping, payroll and HR data;
2. Any working papers that support your compliance work which contain personal data;
3. Any customer data you hold for marketing purposes;
4. Emails and correspondence, both internal and external, since many of these will relate to clients and to their employees and will therefore contain personal data;
5. It's not just electronic data. Any records that are stored in a form that is easily searchable can fall under the remit of regulation.

Data Management - GDPR

How will GDPR affect surveying practices?

In summary:

- You must have knowledge of the data you store and process, its geography (where it resides), security usage and composition:
 - Is it personal, prohibited, client-related or employee-related?
 - How is it captured - is it permitted by law and by the client?
- You must be able to provide information on how the data is used and on the rights of individuals regarding their data.
- You must demonstrate that you are managing personal data in a manner compliant with the regulations and be able to supply, on request, the details of the data you hold and how it has been used.
- You have to be able to delete every instance of an individual's data in compliance with the right to be forgotten (including data held in backups).
- You must offer this data in a format that allows portability to other data processors should the need arise.

Data Management - GDPR

Who Regulates The GDPR?

The Information Commissioner's Office (**ICO**)

Wycliffe House,

Water Lane,

Wilmslow,

Cheshire SK9 5AF

Tel. 0303 123 1113

e-mail: international.team@ico.org.uk

Website: <https://ico.org.uk>

Data Management - GDPR

Breaches

- A personal data breach is defined as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”
- Data breaches must be reported to the national regulator but only where it is likely to result in a risk to the rights and freedoms of individuals. The test to consider is if unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.
- Breaches are typically discovered through access logs, reported thefts, lost equipment or a data security incident that involves personal data. This initial report must be made within 72 hours of having become aware of it. And to clarify - these hours don't stop for weekends and evenings. You'll have longer to compile a full report if required but you must make the ICO aware within those first 3 days.

Data Management - GDPR

What are the maximum penalties?

If your organisation is found to be non-compliant there are fines of up to 4% of its annual worldwide turnover or €20 million, whichever is greater. This is the maximum fine that can be imposed for the most serious infringements (e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts).

There is a tiered approach to fines (e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment).

It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Data Management - GDPR

Best Practice to be compliant with the new GDPR

1. **Conduct a data review:** A data audit to understand risks, access rights, purpose for storing the data, clarifying your rights to ensure you have consent to store the data (more importantly, the right to store the data for the purpose in which you are using it).
2. **Anonymise data** wherever possible.
3. **Encrypt everything** (wherever possible) including Laptops and memory sticks
4. **Create a Breach Response Policy:** Understand the Data Subject Request process: A plan should be in place to handle client's requests for data or changes to this data.
5. **It's more than just personal data:** The GDPR is primarily responsible for personal data. This means that corporate data does not fall under its remit. RICS firmly believes that the surveying profession must treat sensitive commercial data in largely the same way as personal data. A robust data handling policy will encompass all aspects of your organisation's data and in return your client data will be more secure.
6. **Consider the data landscape:** Employee's personal devices, if they are using them for business purposes, fall within the scope of the GDPR so it is important that your organisation's policies include provisions for personal devices to ensure that all employees are compliant.

Data Management - GDPR

Best Practice to be compliant with the new GDPR (Cont'd)

7. **Data storage:** If you store data, remember that GDPR does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that: “Data is to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; **The question an individual / firm needs to consider is why they believe it is necessary to continue to hold personal information).**
8. In practice, it means that firms need to:
 - review the length of time personal data is kept;
 - consider the purpose or purposes the information is held when deciding whether (and for how long) to retain it. For instance; Is there an insurance requirement, industry requirement, or sources that stipulate minimum retention periods, such as local laws etc.
 - securely destroy information that is no longer needed for this purpose, or these purposes; Remember that retained data should only be used for the purpose it was originally collected for. If it is to be used for another purpose make sure there is a legal basis to do so

Data Management - GDPR

What is the difference between a **regulation** and a **directive**?

A **regulation** is a binding legislative act. It must be applied in its entirety across the EU, while a **directive** is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how. It is important to note that the GDPR is a regulation, in contrast to the previous legislation, which was a directive.

Data Management - GDPR

Exercise – 30 mins max.

Everybody to be separated into 4 groups – QS's (Cost Consultants), BS's, Valuers, Property Agency and Property Management. Split the larger groups so, for example there may be 3 QS groups.

1. Each group to nominate a spokesperson and scribe (one and the same person).
2. Each group takes a large sheet of flip chart paper/pen.
3. Each group to be given a sheet with the "Scenarios" and "Issues" on for their respective group.
4. The workshop tutor has a sheet with both the "Scenarios" and "Issues" and the "GDPR points to note" on.
5. The groups to debate what the "GDPR Points to Note" could be for each of the respective Pathways.
6. Each of the spokespersons then present the group's findings at the front of the class and after each presentation the workshop tutor to explain what they have on their sheets.

Data Management - GDPR

Scenario – Building Surveying:

- Partnership D is a small business conducting residential surveys in a local area.
- Its clients include a purchaser of a property from a family with a severely disabled child who have made adaptations to the family home over the years.

Issues:

- In the course of conducting surveys, the partnership will collect large volumes of personal data, both of the clients for the surveys, and the sellers.
- In the case of the family with the disabled child, information regarding health is a 'special category' of personal data.

Data Management - GDPR

Scenario – Cost Consultancy:

- Company E have been in business in the UK for 20 years. As a result of a merger with another firm, they are streamlining their systems and processes and introducing BIM modelling and management through the lifecycle of the CCM process. This involves using a third party SI to ensure all the third party systems operate and interface effectively in order for the data to flow through the end-to-end process.

Issues:

- The processes, data and outputs of the modelling and management tools are likely to be financial rather than personal data.
- There will be significant personal data in relation to the construction stage if details of sub-contractor staff with their wages and other information is captured in the process.

Data Management - GDPR

Scenario – Property Agency:

- Agency B handles sales and rentals through a network of offices in the UK and Spain and a satellite office in Dubai.
- The Agency uses a number of third party tools and systems to process data, including online systems for Anti-Money Laundering (AML) and Know Your Client (KYC) checks, and tenant background checks on behalf of landlords.
- Most of the systems and data are accessible by staff in all offices.
- The systems are being upgraded and some are being migrated to cloud solutions.
- The Agency follows the RICS Professional Statement on Conflicts of Interest and turns down work for potential tenants where it has previously acted for the relevant landlord.

Data Management - GDPR

Scenario – Property Agency (Cont'd)

Issues:

- Data transfers between offices can happen even if the data/application is hosted in one office or location.
- The terms of the contract with the third party providers of tools and services will set out their own approach to security and data protection issues, which may or may not have been negotiated by agency B.
- Cloud services are routinely backed up at locations away from the main data centres (sometimes with large providers). The entire supply chain is not always visible to the end user client but its data (and that of its clients and marketing contacts) may be held and transferred throughout this supply chain.
- The Professional Statement places a positive obligation on RICS professionals and firms to identify and manage Conflicts of Interest (as defined in the Professional Statement). They also impose duty to retain auditable records of any Informed Consents which are obtained.

Data Management - GDPR

Scenario – Property Management

- Company C is responsible for all aspects of FM and property management for the offices of an international bank. As well as the usual building maintenance, repairs and cleaning, this includes CCTV and security, car parking, HSE checks and incidents and the provision of front of house staff.
- The bank flows down its own security and data protection requirements into contracts with all of its suppliers.

Issues:

- Company C provides the services using multiple third parties under contracts for which it acts as agent for the bank. It therefore has no direct contractual relationship with those service providers.
- Data regarding visitors is likely to be stored for ease of admittance after the first visit.
- Health and safety incident reports involve recording the name and any injuries of the individuals involved. This information is kept for six years in the event of litigation.

Data Management - GDPR

Exercise – 30 mins

- Everybody to be separated into groups as before – QS's (Cost Consultants), BS's, Valuers, Property Agency and Property Management. Split the larger groups so, for example there may be 3 QS groups.
- Each group to nominate a spokesperson and scribe (one and the same person).
- Each group takes a large sheet of flip chart paper/pen.
- See the next slide for the requirements.
- Each of the spokespersons then present the group's findings at the front of the class and after each presentation the workshop tutor to possibly discuss.

Data Management - GDPR

Exercise – Cont'd

Knowledge and Understanding of the sources of information and data

Identify information and data systems applicable to your area of practice

Identify methodologies and techniques most appropriate to collect and store data in relation to your area of practice

- Break out into Groups based upon your individual Pathways
- Identify the sources of information and data systems that you and your company use and identify methodologies and techniques most appropriate to collect and store data in relation to your area of practice

Data Management - GDPR

You should now:

- Know about GDPR.
- Have knowledge and understanding of the sources of information and data.
- Be able to identify information and data systems applicable to your area of practice.
- Identify methodologies and techniques most appropriate to collect, collate and store data in relation to their area of practice.

Data Management - GDPR

Useful Links

- <https://www.rics.org/uk/footer/gdpr/gdpr-factsheets/>
- <https://www.rics.org/uk/footer/gdpr/>