Institute and Faculty of Actuaries

Preparing for the GDPR

Martin Sloan, Partner, Brodies LLP
Des Hudson, Chair, Regulation Board

9 March 2018

What is your main practice area?

a) Life Assurance
b) General Insurance
c) Pensions
d) Finance and Investment
e) Enterprise Risk Management
f) Health and Care
g) Resource and Environment
h) Other

Which of the options below best describes the type of organisation that you work for?

a) Actuarial consultancy
b) Insurance company or reinsurer
c) Bank or Building Society
d) Investment Firm
e) Public body or Regulator
f) Other

Where is your role based?

a) Within the UK

b) Outside of the UK

Institute and Faculty of Actuaries

What is your/your firm's state of readiness in terms of preparation for GDPR coming into effect on 25 May 2018?

a) 100% ready

b) Still work to do

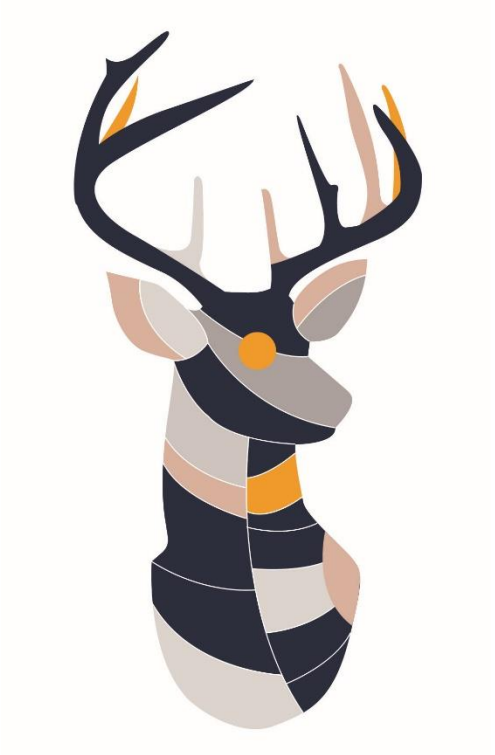
c) Not ready at all

d) Don't know

Institute and Faculty of Actuaries

Outline

- Data Protection basics
- The General Data Protection Regulation
- Preparing for the GDPR



Institute and Faculty of Actuaries

Data protection basics

Institute and Faculty of Actuaries

Data Protection basics

Current data protection law

- 1995 EU Data Protection Directive
- Applies to **controllers** who **process** data that is **personal data**
  - **"controller"** – the legal entity that determines the purpose and means of the processing of personal data
  - **"processor"** – someone who processes personal data on behalf of the controller (NB an employee is not a processor)
  - **"process"** – essentially anything you do with personal data (including simply holding it in a file/in storage)
  - **"personal data"** – any information relating to an identified or identifiable living individual.

Are you a controller or a processor?

- **Actuaries and current data protection law**

- Your organisation may be a **controller**
  - responsible for compliance with data protection law (eg DPA)
  - responsible for any processing carried out by its **processors**

- Or your organisation may be a **processor**, processing on the instruction of another organisation

- Professional advisors generally viewed as being **controllers**

- Scheme actuaries – personal appointment, so:
  - scheme actuary is him or herself a **controller**
  - But may be a **joint controller** with their firm

Institute and Faculty of Actuaries

Not long to go…

77 days

53 working days

Institute and Faculty of Actuaries

Background

- The biggest shake-up of data protection law in nearly 25 years
- The General Data Protection Regulation (GDPR)
  - New EU-wide data protection law which will have direct effect
  - Enters into force on 25 May 2018
  - Greater consistency of regulatory treatment
  - Stronger and more coherent data protection framework
  - Backed by strong enforcement
- Supplemented by national implementing legislation
- Applies in the UK notwithstanding Brexit
- ePrivacy reform on the horizon too

Why does it matter?

- **Compliance risk**
  - it's the law
  - Regulatory action
- **Financial risk**
  - Monetary penalties for non-compliance
  - Clean-up costs, management time, compensation claims
- **Operational risk**
  - Stop processing orders; regulatory audits and investigations
- **Reputational risk**
  - Adverse publicity
  - Loss of trust

The GDPR – an overview of what's changing

Institute and Faculty of Actuaries

Evolutionary

Some concepts remain broadly similar

- **Key concepts** – personal data, sensitive personal data, processing, data controllers, data processors etc
- **Data protection principles** – recognizable, but explicit reference to both transparency and accountability
- **Conditions for processing** – similar, but some changes
- **Data subject rights** – broadly recognizable (subject access, rectification, processing restrictions), but there are some new ones
- **International transfers**
- **Basic data security obligations** – BUT see new data security breach notification requirements
- **The ICO** – still a UK national supervisory authority

What's changing?

- **Transparency** – enhanced fair processing transparency requirements (including tighter rules on consent)
- **Accountability** – obligation to demonstrate compliance; use of privacy impact assessments; training; policies; data protection officers
- **Administration** – increased administration and record keeping
- **Data subject rights** – enhanced rights including subject access, increased 'rights to be forgotten' and data portability
- **Organisational principles** – data protection by design and by default
- **Breach notification** – mandatory breach notification for certain breaches
- **Sanctions** – increased fines and new enforcement powers

Who is subject to GDPR?

- Within the EU – organisations **established** in the EU
- Outside the EU – organisations established **outside** the EU where the processing relates to:
  - offering goods/services to individuals in the EU
  - monitoring the behaviour of individuals in the EU
- Establishment = effective and real exercise of activity through stable arrangements
- **Processors** – GDPR imposes new obligations

GDPR: data protection principles

1. •Processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. •Collected for specified, explicit and legitimate purposes and not further processed for incompatible purposes (**purpose limitation**)
3. •Adequate, relevant and limited to what is necessary (**data minimisation**)
4. • Accurate and, where necessary, kept up to date (**accuracy**)
5. •Kept in a form which permits identification of data subjects only for as long as necessary (**storage limitation**)
6. •Processed in an appropriate manner to maintain security (**integrity and confidentiality**)
7. •Controller shall be responsible for and demonstrate compliance with these principles (**accountability**)

Accountability

Data Governance

- Controllers are not only expected to comply with the GDPR – they are expected to be able to **demonstrate** that they comply
- New responsibilities include:
  - Implementing ‘appropriate and effective measures’ for compliance including appropriate data protection policies
  - Data protection by design and default – building DP compliance (eg data minimisation) into processing processes and activities
  - Conducting data protection impact assessments for processing considered to be ‘high risk’
  - Detailed requirements to keep records of processing activities
  - Express obligation to co-operate with regulators

Accountability

Data Governance – Data Protection Officers

- Mandatory for controllers and processors whose core activities involve
  - Regular processing of sensitive personal data
  - Regular/systematic data monitoring of data subjects on a ‘large scale’
- Can be on group-wide basis so long as DPO is ‘easily accessible’
- DPO must
  - have professional qualities and expert knowledge
  - be allowed to perform responsibilities in an independent manner
  - be supported and properly resourced
- Conflicts of interest
- DPO role – general advisory; compliance monitoring; training and awareness; audits; privacy DPIAs; and dealing with regulators
- Not personally responsible for compliance
- DPO may be an employee or a contractor

Accountability

Data protection impact assessments

- Application
  - GDPR requires DPIAs for “high risk” processing
  - WP29 recommends DPIAs as an accountability tool in other situations
  - WP29 considers the list of activities in article 35(3) to be non-exhaustive
  - If no DPIA then you should document why it is not required
- Existing processing
  - No need to carry out for existing processing – unless change to risk
- Timing, personnel and consultation
  - Early stage and reviewed periodically (at least every three years)
  - If you have a DPO then they must be involved
  - Obtain views of data subjects (and if not document why)
- Publication
  - WP29 recommends that data controllers should publish DPIAs

Transparency

Processing on the basis of consent

- Onus on controller to demonstrate valid consent has been given
- Consent must be **freely given**, **specific**, **informed** and **unambiguous** and requires **affirmative action**
  - Ticking a box (eg opt-in) or choosing technical settings etc
  - Not silence, pre-ticked boxes or inactivity
  - Clear and plain language
- No bundled consent
- It must be as easy to withdraw consent as to give it
- Gives rise to stronger rights – is there a better legal basis?

Transparency

Privacy/information notices

- Controllers must provide data subjects with more information, including:
  - Legal basis for processing
  - If legitimate interests are relied on, what those are
  - Details of any international data transfers
  - Data retention periods (or criteria used to determine them)
  - The existence of the various data subject rights
  - The right to withdraw consent at any time
  - The right to complain to the ICO
- Must be concise, transparent, intelligible and in an easily accessible form
- When?
  - At the point of data collection
  - Or within one month if data not collected from the data subject

Transparency

Enhanced rights for individuals

- **Right of erasure/right to be forgotten** – individuals can ask for their data to be erased where the processing no longer satisfies the GDPR

- **Data portability –** requires controllers to provide data to other controllers in a common file format on request where data was provided by individual and processing is based on contract or consent

- **Data Subject Access Requests** – changes to current rules
  - One month rather than 40 days
  - No right to charge (unless excessive/repetitive requests)
  - Rights to receive additional information about processing

Data processors

Direct obligations and mandatory contract clauses

- Processors will have direct obligations under the GDPR
- Includes obligations relating to:
  - Record keeping
  - Co-operation and consultation
  - Sub-processors
  - Data security
  - Data breach notifications and data subjects
  - Sanctions for breaches
  - DPO
- Specific requirements for contracts with processors – no grandfathering of current contracts

Data breach notifications

Breach notification now on statutory footing

- Applies to both data controllers and data processors
- Data controllers:
  - Duty to notify the supervisory authority within 72 hours of becoming aware of a breach *"unless unlikely to result in a risk for the rights and freedoms of individuals"*
  - Notification to affected individuals without 'undue delay' unless:
    - Unlikely to result in a high risk for the rights and freedoms of data subjects
    - Appropriate protections were in place at the time of the incidence (for instance - the data was encrypted)
    - It would be disproportionate
    - WP29 draft guidance
- Data processors: duty to inform data controllers without 'undue delay'

Regulation and enforcement

Increased powers for regulators

- Powers include:
  - Investigative powers:
    - Information disclosure orders
    - Conducting data protection audits
    - Power of access to personal data
    - Power to access premises/equipment
  - Corrective powers:
    - powers to fine
    - ban processing
    - suspend international data flows
- Explicit obligation to co-operate with regulators on request

Regulation and enforcement

Fines for non-compliance

- Substantially broader than ICO's current powers to fine:
  - No requirement for substantial distress/harm
  - Potential to apply to administrative errors
  - Significant increase in maximum fines
  - Also applies to processors

- **But** power is discretionary:
  - Fines must be "*proportionate, effective and dissuasive*"
  - Article 79 sets out relevant factors
  - NB consistency mechanism

Preparing for the GDPR

Institute and Faculty of Actuaries

Preparing for GDPR

Basic preparatory steps

- ICO has issued a checklist with 12 steps to take for GDPR preparation

- Initial steps:
  - Resource
  - Data Mapping
  - Data minimisation
  - Review processing justifications
  - Contract reviews

Institute and Faculty of Actuaries

Area	Requirement/Impact	Action
General		
Resourcing	Do you need to appoint/should you appoint a DPO? Increased requirements of GDPR will place additional compliance obligations on organisations.	Ensure responsibility for GDPR is clear at board level. Appoint a DPO quickly (if you're appointing one) Properly resource ongoing compliance. Is there sufficient expertise within the organisation? Consider establishment of central compliance function with responsibility for handling regulatory queries, DSARs/other individual requests, data security breaches, training etc
Data audit	Any GDPR compliance programme needs to be built on a complete picture of what data is being processed, why it is being processed and by whom it is being processed to establish where the organisation is not GDPR compliant and to establish a prioritised action plan	Conduct a data audit, remembering that the audit should catch processing
Extra-territorial reach	Extra territorial impact will catch processing outside EU which targets EU citizens even by organisations that have no EU presence or nexus	For groups operating outside EU analyse any processing by non-EU group companies for GDPR compliance. Consider whether measures can be taken to avoid unnecessary GDPR reach.

Area	Requirement/Impact	Action
Accountability and Administration		
Accountability	More generally, organisations will need to implement appropriate policies and implement measures that demonstrate compliance	Consider the adequacy of policies and measures. They may need revamped and you may need new ones.
Transparency	GDPR requires more information to be included in privacy notices	Privacy notices will need to be reviewed and updated. Use layered and 'just in time' notices
Consent based processing	Requirements for consent based processing are tighter. Likely to impact particularly in areas such as marketing	Will existing consents be valid for GDPR purposes? If not, will they need refreshed or can processing for grounded on an alternative basis?
Data retention	Requirement for greater transparency mean that organisations will face greater scrutiny around data retention and destruction practices.	Ensure that organisation has appropriate data retention and destruction policies and procedures and that they are being actioned both for new and legacy data
Data Protection Impact Assessments	DPIAs will be on a statutory footing under GDPR.	Organisations must be prepared to carry out DPIAs for 'high risk' processing and those operations for which DPIAs are proscribed. Develop DPIA process and methodology and appropriate policies and procedures (see earlier).
Record keeping	Many organisations will be required to keep records of processing being carried out	Review record keeping to ensure adequacy. Consider if exemption applies (organisations with less than 250 employees provided certain other conditions are met).

Area	Requirement/Impact	Action
Security		
Data security	Although data security standards are broadly the same, the requirements are more explicit - and the penalties for data security breach are greater	Consider whether current data security standards are adequate.
Data breaches	GDPR introduces requirements for mandatory data security breach notifications	Introduce clear policy and procedure for internal reporting of data security breaches. Establish central breach management unit
Commercial		
Contracts	New requirements for data processing agreements	Review data processing agreements which will run post May 2018 and update contract templates
Technology refresh	New GDPR requirements may require additional functionality of legacy IT systems	Review existing IT. is it up to scratch? Consider contractual position before engaging with suppliers.
Procurement	Ensure that GDPR is factored into new IT procurements	Ensure GDPR compliance is factored into procurement decisions. Consider if a DPIA is required.

Key Actions

- Identify **your team** and **plan your strategy** for compliance
- Create an **information asset register** – what personal information and where, why, how and with whom do you process it
- Understand your **status** – controller, joint controller or processor
- Review your **template documentation**
- Review your **privacy notices**
- Review your **processes and systems** for dealing with data subjects rights
- Implement **data governance policies** and measures and training to ensure your staff operate in accordance with GDPR
- Review **data handling arrangements for investigations**
- Review your **supply chain arrangements** with **data processors**, such as IT and outsourced service providers
- Review your **data sharing arrangements** with third parties
- Review the **data you hold** and your **data retention policies** and **practices**

Questions…

Institute and Faculty of Actuaries