Introduction – Who We Are

- Specialist providers of FCA compliance and training to the General Insurance Industry
- Trading since 2002
- We ***only*** deal with General Insurance
- Professionally qualified and experienced
- Plain English, ***straight to the point*** … no jargon!

What We Will Cover Today

- Some background to the Regulation
- The definition of 'personal data'
- What is meant by 'protection'
- Establishing your legal basis for processing data
- New rights for individuals
- The risks to your business
- The potential impact on marketing activities
- Governance / internal systems and procedures

Learning Objectives

- Understand the background to GDPR and why the law is changing
- Understand some of the key areas and activities that will be affected by the change and how it relates to the General Insurance Industry
- Understand how your business may be affected
- Understand the consequences of falling foul of the new regulations

Background

- GDPR comes into effect 25th May 2018
- It replaces existing Data Protection legislation
- It is a Regulation not a Directive
- Member states will introduce additional legislation to supplement GDPR

Background

The Aim is:

- To ensure the same standard of Data Protection across all EU Member States
- To strengthen the rights of individual Data Subjects
- To ensure the 'free flow' of data between EU Member States

Background

- Supervisory authorities will have increased powers (bigger fines!)
- Reporting of breaches will become mandatory
- Non EU countries will have to comply if they want to offer goods or services in the EU
- Marketing may pose extra risks

What is 'Personal Data'?

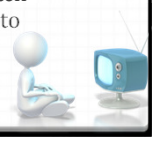
- **In the GDPR, 'Personal Data' is defined as:**

"any information relating to an identified or ***identifiable*** natural person ('data subject');

an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic or social identity of that natural person"

What is 'Personal Data'?

- The GDPR definition of 'Personal Data' is wider than the definition under previous legislation
- It is designed to take account of new technologies and ways of doing business that have developed since data protection was first introduced (when we used to watch analogue TV and dial up via a modem to connect our PCs to the internet!)



‘Special Categories’ of Data

- Personal data relating to the following are classed as ‘Special Categories’ of data:
  - Racial or ethnic origin
  - Political opinions, religious or philosophical beliefs
  - Trade union membership
  - Genetic and biometric data
  - Health
  - Sex life or sexual orientation

‘Special Categories’ of Data

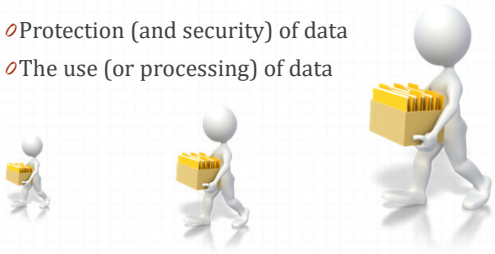
- Processing of special categories of data is prohibited under GDPR
- It is up to individual EU Member States to decide which types of organisations have exemptions to this rule
- In the Data Protection Bill currently going through Parliament in the UK, insurance is one of these exemptions

Criminal Convictions & Offences

- Processing of personal data relating to criminal convictions and offences also requires an exemption

Data **Protection**

- In our view, the subject of **Data Protection** should be divided in two:
  - Protection (and security) of data
  - The use (or processing) of data



Data Protection

- **Protection** is about keeping data safe and secure
- **Processing** is about what you do with the data:
  - How you collect and store it
  - What you use it for
  - Who you pass it to

- Firms need to address both areas

Legal Basis for Processing Data

- Under GDPR, a firm must have a valid Legal Basis for processing data
- There are six legal bases for processing data
- It's not all about consent!

Legal Basis for Processing Data

- Consent
- Necessary for performance of a contract
- Where there is a legal obligation
- Vital interests
- Public interest
- Legitimate interest

Legal Basis

- Your processing activities should be split into:

Insurance **Marketing**

Legal Basis

- The legal basis you are likely to rely on for **insurance** is **"necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"**

Legal Basis

- The legal basis you are likely to rely on for **marketing** is **"necessity for the purposes of the legitmate interests pursued by the controller"** or **"consent"**

Individuals get new rights under GDPR

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

The right to be informed

- Individuals have the right to know that personal data concerning them are collected, used, or processed and to what extent
- They must be given specific information about this and it must be in a clear and accessible format, in easy to understand and plain language

The right of access

- Individuals have a right to access the data you hold on them – free of charge – previously many companies charged a nominal fee for this

The right of rectification

- Individuals have the right to request any information you hold on them be corrected

The right of erasure

Individuals have the right to request the information you hold on them be erased, where specific grounds apply

The right of erasure

- The data is no longer necessary in relation to the purposes for which they were collected or processed
- The data subject withdraws consent or objects to processing and there is no other legal ground for processing
- The data has been unlawfully processed

The right to restrict processing

- Individuals have the right to restrict processing under certain conditions

The right to restrict processing

- Where the accuracy of data is contested
- Where processing is unlawful
- Where the data is required for legal reasons
- Where the individual has objected to processing pending verification of whether the legitimate grounds of the controller override those of the data subject

The right to data portability

- Individuals have a right to data portability where the processing is based on consent or performance of a contract **and** is carried out by automated means
- This means they can request their data be supplied in a machine-readable format and transmitted from one controller to another, where technically feasible

The right to object

- Individuals have the right to object to processing of personal data for direct marketing purposes

Rights in relation to automated decision making and profiling

- Individuals have the right not to be subject to a decision based solely on automated processing (including profiling)
- This right doesn't apply where the processing is necessary for performance of a contract, but individuals will still have the right to request human intervention

Right to complain to the supervisory authority

- Individuals have the right to complain to the GRA and you must tell them about this

Moneysupermarket

- **Fined £80,000**
- They sent over 7 million emails updating customers with new terms and conditions and included the text "we hold an email address for you which means we could be sending you personalised news, products and promotions. You've told us in the past that you prefer not to receive these. If you'd like to reconsider, simply click the following link to start receiving our emails"

Moneysupermarket

- **ICO Head of Enforcement said:**

"Organisations can't get around the law by sending direct marketing dressed up as legitimate updates.

When people opt out of direct marketing, organisations must stop sending it, no questions asked, until such time as the consumer gives their consent. They don't get a chance to persuade people to change their minds"

Moneysupermarket

- **He also added:**

"Emails sent by companies to consumers under the guise of 'customer service', checking or seeking their consent, is a circumvention of the rules and is unacceptable. We will continue to take action against companies that choose to ignore the rules"

Morrisons Supermarkets

- **Fined £10,500**
- They sent emails to people who had previously opted out of receiving marketing related to their Morrisons More card.
- The emails invited customers to change their marketing preferences to start receiving money off coupons, extra More Points and the 'latest news' from Morrisons.

Morrisons Supermarkets

- **The Deputy Commissioner said:**

"It is vital that the public can trust companies to respect their wishes when it comes to how their personal information is used for marketing.

"These customers had explicitly told Morrisons they didn't want marketing emails about their More card. Morrisons ignored their decision and for that we've taken action"

Flybe

- **Fined £70,000**
- They sent more than 3.3 million emails to people who had told them they didn't want to receive marketing emails.
- The emails, with the title 'Are your details correct?' advised recipients to amend any out of date information and update any marketing preferences. The email also said that by updating their preferences, people may be entered into a prize draw.

Flybe

- **ICO Head of Enforcement said:**
- "Sending emails to determine whether people want to receive marketing without the right consent, is still marketing and it is against the law."
- "In Flybe's case, the company deliberately contacted people who had already opted out of emails from them."

The Lead Experts Limited

- **Fined £70,000**
- Responsible for over 100,000 nuisance calls
- They said they had bought people's contact details from another company and then paid it to carry out the calls
- An ICO investigation found that The Lead Experts were responsible for ensuring they had the necessary consents to make the calls.

The Lead Experts Limited

- **ICO Head of Enforcement said:**
- "Companies cannot hide behind paying another firm to make the calls for them. They must take responsibility and, ultimately accept the consequences if they break the law"

Taking Marketing Seriously

- Marketing activities will be under much greater scrutiny than ever before
- In the UK, many existing marketing practices were already banned under the Privacy and Electronic Communications Regulations 2003 (PECR) but not robustly enforced
- PECR implemented European Directive 2002/58/EC, also known as 'the e-privacy Directive'

Right to Object

- All Data Subjects have the right to object to direct marketing under PECR and GDPR
- This right should be explicitly brought to their attention, and presented clearly and separately from any other information

Right to Object

- GDPR states that a firm must inform a Data Subject of this right at the time of the first communication
- This means that when a firm collects data it must give the Data Subject options about whether to receive Marketing or not
- Effectively, this means they must Opt-in

Legal Basis for Marketing

- Under GDPR, a firm must have a valid Legal Basis for its Marketing activities
- The Legal Basis is likely to be either **Legitimate Interest** or **Consent**

Legitimate Interest

- GDPR explains the Legal Basis of **Legitimate Interest** as "*Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, expect where such interests are overridden by the interests or fundamental rights and freedoms of the data subjects which require protection of personal data, in particular where the data subject is a child*"

Legitimate Interest

- GDPR tells us that "*The processing of personal data for direct marketing purposes may be regarded as carried out for a **legitimate interest***"
- We take this to mean in the UK a firm can market to its own Customers about products & services they have shown an interest in previously, as they are able to now

Legitimate Interest

- However, they must include an unsubscribe option on emails, a STOP for texts, or inform the Data Subject they can opt-out over the telephone or if contacting by post
- This should satisfy the Right to Object requirement

Legitimate Interest

- Best practice may be that when contact is made with the Data Subject (for example at their next Renewal or at the time of a Mid-Term Adjustment), the Marketing preferences of the individual are verified regarding future communications – essentially obtaining their Consent

Consent

- The most used Legal Basis for Marketing is likely to be **Consent**
- GDPR states this Legal Basis as *"**The Data Subject has given consent to the processing of his or her personal data for one or more specific purposes**"*

Conditions of Consent

- A firm must be able to demonstrate that a Data Subject has given their Consent
- This means keeping records – you may need to review what options your software house(s) has in place for this

Conditions of Consent

- The Data Subject can withdraw their Consent at any time, and should be informed of how to do so
- When obtaining Consent for Marketing purposes a firm should ensure Customers are actively opting-in

Conditions of Consent

- An important condition of Consent is that it must be "unambiguous", and must be confirmed "by a statement or by a clear affirmative action"
- This means the use of pre-ticked boxes on websites are not permitted

Conditions of Consent

- A firm should ensure that each method of Marketing (mail, email, call, automated call, text, fax etc.) is separately consented to, allowing the Data Subject to decide by which methods they will accept Marketing information

Conditions of Consent

- Consent therefore should be separate from other terms and conditions
- Best practice might mean having a separate page on a website for an online sales process
- Sales scripts may need to be extended to include questions about Marketing preferences

Other Firms

- A firm will not be able to sell its data to another firm, or share it for Marketing purposes without specific Consent from its Data Subjects
- Firms should also take care using data they have obtained from other firms. If they wish to use it for marketing, they will need to be sure the data subjects have given consent.

Marketing Methods

- The EU Privacy and Electronic Communications Regulations are expected to be updated in line with GDPR and should be announced in good time before
- PECR explains what the specific rules are for Email, Text, Fax & Telephone Marketing

Governance

- In this section we are going to look at some of the systems and procedures you will need in place to comply with GDPR

Governance

You will need:

- Record of Processing Activities
- Privacy Notice
- Systems and procedures to deal with subject access requests and reporting of breaches

Governance

- Under GDPR, you will no longer be required to register as a Data Controller or Data Processor with the GRA
- However, you may still need to pay a fee

Record of Processing Activities

- You will need a written record of your processing activities (to be made available to the GRA on request)
- This is effectively a Data Protection Policy but it must contain certain information

Record of Processing Activities

Required information:

- Name and contact details of the controller, and where applicable the DPO
- The purposes of the processing
- A description and categories of data subjects and of the categories of personal data

Record of Processing Activities

Required information:

- The categories of recipients to whom the personal data have been or will be distributed
- How long you intend to keep the different categories of data

Record of Processing Activities

Required information:

- General description of your IT security measures, including back-up procedures, encryption and who has access to data

Record of Processing Activities

- You may also want to include in this document what **legal basis** you are relying on for processing data
- It's not a requirement of GDPR to include it but we recommend you do

Privacy Notices

- You don't have to use a Privacy Notice but GDPR requires that certain information must be given to data subjects and this must be:
  - Easily accessible
  - Easy to understand
  - Written in clear and plain language

A Privacy Notice is a good way to do this.

Privacy Notices

- The information you need to provide in a Privacy Notice is very similar to the information you need to include in your record of processing activities:
  - Who you are;
  - What you will do with their data;
  - Who you will pass it to; and
  - How long you will keep it for.

Privacy Notices

Your privacy notice should contain:

- Name and contact details of the **controller**;
- Name and contact details of the **DPO** (where applicable);

Privacy Notices

Your privacy notice should contain:

- The purposes of the processing
- The legal basis for processing
- The recipients (or categories of recipients) of the personal data
- How long the data will be stored

Privacy Notices

You must also tell the data subject:

- They have a right to access the data you hold on them (free of charge)
- They have the right to request the information you hold on them be corrected or erased
- They have the right to restrict or object to processing

Privacy Notices

You must also tell the data subject:

- They have a right to data portability
- Where processing is based on consent, they have a right to withdraw this at any time
- They have the right to complain to the GRA

Other Governance Issues

Other Governance Issues include:

- Appointing a DPO
- Privacy Impact Assessments
- Subject Access Requests
- Reporting of Breaches

Appointing a DPO

- There is no requirement for most small - medium sized insurance brokers to appoint a Data Protection Officer

Appointing a DPO

Data Protection Officers are required for:

- Public authorities
- Firms with **large scale** data monitoring as their core activity (targeted ad companies)
- **Large scale** processors of special categories of data or data relating to criminal convictions

Data Protection Officers

- Firms should have a senior member of staff responsible for Data Protection issues, but should **not** call this person a "***Data Protection Officer***" unless they are one

Privacy Impact Assessments

- Supervisory authorities have to establish and publish a list of the kind of processing operations which require a Data Protection Impact Assessment

Privacy Impact Assessments

- In the GRA guidance on DPIAs (October 2017), no data processing operations were identified, for which a DPIA is mandatory

Privacy Impact Assessments

- In any case, they are only required where processing operations could result in a **high risk to the rights and freedoms of natural persons**

Privacy Impact Assessments

- Examples given in the GDPR include:
  - Where data is being processed using new technologies
  - Where profiling operations are likely to significantly affect individuals
  - Where there is large scale monitoring of a publicly accessible area

Subject Access Requests

- Data subjects have the right to request a copy of the personal data that is being processed
- You must provide this free of charge unless the request is 'unreasonable' in which case you can charge a reasonable fee based on admin costs

Subject Access Requests

- You will need systems in place to ensure you can respond appropriately to these requests
- Your systems should allow you to easily locate and extract personal data
- This includes data that has been archived and/or backed up (but not deleted)

Subject Access Requests

- It is good practice to manage expectations and acknowledge the request, informing the client of the expected date of response
- You should respond within one month, or if this is not possible, you need to respond with the reasons why
- If the request is made electronically, you should respond electronically

Subject Access Requests

You don't have to supply original documents but you must give the requester:

- A copy of any information you hold on them,
- The reason(s) for processing it
- Details of the source of the data and whether it is being passed to other organisations
- Information about the reasoning behind any automated decisions

Reporting of Breaches

- Data breaches must be notified to the supervisory authority as soon as possible (latest 72 hours after becoming aware of it), **unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons**

Reporting of Breaches

- **What you need to tell the GRA:**
  - The nature of the breach, including where possible the categories and number of data subjects concerned and the categories and approximate number of personal records concerned
  - The name and contact details for the DPO or whoever is in charge of Data Protection at your firm

Reporting of Breaches

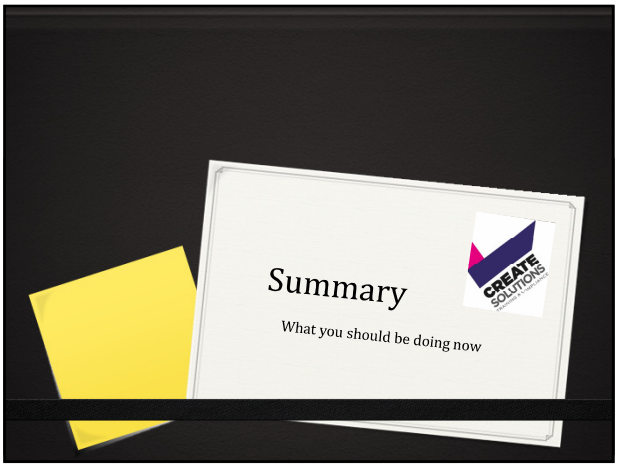
- **What you need to tell the GRA:**
  - The likely consequences of the breach
  - Measures you have taken or propose to take to address the breach, including, where appropriate, measures to mitigate any potential adverse effects

Reporting of Breaches

- **What you need to tell the Data Subject:**
  - The nature and potential consequences of the breach
  - Measures you have taken or propose to take to address the breach, including, where appropriate, measures to mitigate any potential adverse effects
  - The name and contact details for the DPO or whoever is in charge of Data Protection at your firm

Enforcement

- **Fines up to 2% of global turnover (or 10M Euros) or up to 4% of global turnover or £20M Euros)**
  - Depending on the type of infringement and category and any action taken by the firm before or after an incident



What you should do now

- **Raise Awareness:**
  - Make sure that key decision makers and senior managers in your firm know the law is changing and understand the implications
  - Make sure this information is cascaded down to appropriate staff and they are trained in the new rules

What you should do now

- **Carry out an Information Audit:**
  - Work out and document what personal data you hold, what you do with it, where it came from and who you share it with.
  - Identify and document your legal basis for processing data
  - Create your Record of Processing

What you should do now

- **Review your Privacy Notice:**
  - Make sure it contains the necessary information and that it is clear and easy to understand
  - Make sure you ask for consent for sending marketing material separately and that it specifies what type of marketing (text, phone, email, mail etc). Don't use pre-ticked boxes.

What you should do now

- **Review your internal systems and controls:**
  - You will need policies and procedures for responding to various requests from Data Subjects
  - You will need policies and procedures for handling data breaches

What you should do now

- **Review your internal systems and controls:**
  - You will need to put someone in charge of Data Protection
  - You will need to review your IT systems to ensure you have robust data security