General Data Protection Regulation - Explained

Bernard Cogan & Bobby Gould CUNA Mutual Group
ACE Conference & AGM 2017 12th May – 13th May 2017
Copthorne Hotel (Birmingham)
Are you familiar with GDPR – Don't worry most aren't

<table>
<thead>
<tr>
<th>Are you familiar with the GDPR?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>YES</strong> 19%</td>
</tr>
<tr>
<td><strong>NO</strong> 81%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Do you think that the GDPR affects your organisation?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>YES</strong> 57%</td>
</tr>
<tr>
<td><strong>NO</strong> 43%</td>
</tr>
</tbody>
</table>

Your organisation has a process in place for data destruction with:

- **DESKTOPS** 55%
- **STORAGE SYSTEMS** 42%
- **MOBILE DEVICES** 29%
- **CLOUD** 8%
General Data Protection Regulation – GDPR
Introduced to harmonise the data privacy regulatory environment in the EU

- Becomes Law in **May 2018** for all Data Processors & Controllers including Credit Unions
- Retains the same core rules as the Data Protection Act 1998
- Strengthens individual persons rights around their data
- Applies to any entity offering goods or services in the EU or processing data concerning EU citizens
- Applies to both processors and data controllers
- Provided for more information to individuals about the processing of their data
- Introduces harder obligations to notify security breaches
- Tighter rules on transferring data EU citizens outside the EU
- Imposes heavy fines for breaches of the new rules and allows individuals to sue for damages.
Let’s Just Remind ourselves

What is data privacy about?

✓ Persons (Members) have rights around the use and storage of their data, to whom it can be disclosed, sent to etc. Credit Unions collect and keep lots of information about their members.

✓ Data Privacy laws enable credit unions & businesses to use personal information for legitimate business purposes whilst at the same time ensuring the privacy and rights of an individual are preserved.

✓ Data Controllers* must protect an individual’s privacy through putting in place controls around personal information, “treat personal data like you would cash”

✓ Currently the UK Data Protection Act 1998 – adapted in different ways across the EU.

*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.
Two Types of European Legislation

**EU Directives:**
- Individual EU Countries implement directives into local laws
- UK Data Protection Act 1998 came about from an EU Directive
- Directives often put into law at different times with local changes etc.

**EU Regulations:**
- These have Immediately effect in each EU Member State
- Become law as they are with no local changes
- **General Data Protection Regulation** is an EU Regulation and comes into effect in May 2018
- GDPR is first major European data protection law update since 1995 and replaces national laws
Yes but What about BREXIT?

The GDPR will apply in the UK from 25 May 2018. The UK Government has confirmed that the UK’s decision to leave the EU will not affect the commencement of the GDPR. In any case GDPR applies to businesses outside the EU offering goods and services in the EU.

Karen Bradley, Secretary of State

“it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public’

This statement has since been welcomed by Elizabeth Denham, Information Commissioner as reflected on the ICO’s
What does the Information Commissioners Office Say?

“The GDPR gives companies the requirement to understand the risks that they create for others, and to mitigate those risks.

“Its not about seeing the new law as box ticking exercise, but rather to create a framework that can be used to build a culture of privacy that pervades an entire organisation.”

“The GDPR mandates organisations to put into place comprehensive but proportionate governance measures.”

“It means a cultural change to an organisation, accountability cannot be bolted on, it needs to be a part of the company’s overall systems approach to how it manages and processes personal data.”
GDRP Penalties

- **GDPR** sets out a Two-tiered approach to fines depending on the type of non-compliance

**Lower Tier includes breach of**
- the rules relating to processor contracts
- record keeping obligations and processing security requirements

Fine = **the higher of €10 000 000 or 2% of global annual turnover**

**Upper Tier include breaches of**
- the basic principles for processing personal data including conditions for consent
- infringing data subjects' rights
- unlawful transfers to countries outside the EEA

Fine = **the greater of €20 000 000 or 4% global annual turnover**
General Data Protection Regulation - Key Changes

Data Processors
 ✓ Obligations for both the data Controller & Processers - e.g. IT providers

The requirements for a valid consent have become stricter
 ✓ Individuals must be informed of how their information will be collected, processed and stored and for what purposes it will be used.
 ✓ Consent for each purpose must be explicitly given.

Data control, risk management and prevention
 ✓ As well as appropriate documentation will be key to a good data strategy & governance

Codes of conduct and certification mechanisms
 ✓ Privacy of personal data must be built into all systems and processes for collecting
More key changes

**Definition of Personal and Sensitive Data:**

- The GDPR now defines personal data to include an *identification number*, location data and an online identifier, genetic data and biometric data.

- **Consent:**
  Persons can *withdraw their consent* at any time for their data being used.

- **Privacy Notices**
  Processing the data and the *period of time* for which the data will be retained.

- **Right to Rectification,**
  Erasure, Restriction, Data Portability, the GDPR is designed to give data subjects more control by giving persons the *opportunity to object to processing* which is based on the legitimate interest of the controller or a third party.
Appointment of DPO & The Role

Although the GDPR specifically requires the appointment of a DPO in certain circumstances they advise that it best practice for all to have one appointed.

Job Description:

1. **Legal knowledge** together with information security knowledge and skills
2. Understanding of **risk management** and risk assessments
3. Familiarity with codes of **conduct for industry sector**
4. Understanding of compliance standards and data marks
5. Carry out internal audits information security standard
6. Able to coordinate and **advise on data breaches** and notification
7. Able to make a cyber security incident response process work.
8. Leads co-operation with supervisory authority
Accountability and what it means
Principles to Processing of Personal Data

The controller shall be responsible for, and be able to demonstrate compliance

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and, where necessary, kept up to date
5. Retained only for as long as necessary
6. Processed in an appropriate manner to maintain security
Taking Principle 6

After the Credit Union has appointed a Data Controller (or decided not to) and considering Principle 6

• Ensure a level of security appropriate to the nature of the data and the harm that might result from a breach of security
• The data controller must take reasonable steps to ensure the reliability of any employees who have access to the personal data
• Be clear about who in your organisation is responsible for ensuring information security
• Make sure you have the right physical and technical security, backed up by robust *policies and procedures* and reliable, well-trained staff and
• Be ready to respond to any breach of security swiftly and effectively
• Report to the Board regularly, perhaps monthly for the first year of GDPR and strive to change the culture of the credit union around data protection.
What next when considering the GDPR

**Roles & Responsibilities – Who?**

- Who is responsible overall for information security?
- Who will be responsible for meeting legal, regulatory & GDPR obligations?
- Who will be responsible for oversight of legal, regulatory & GDPR obligations?
- Who is and will be responsible for contracts with data processors?
- Who is responsible for identifying and managing privacy risks?
- Will the DPO be a member of the Board,
More Considerations

1. Firms shouldn’t keep data forever – unless of course it’s to ensure that they don’t contact someone who has expressly said that they don’t want to be contacted in the future and not having such information could lead to them being contacted again by accident.

2. Credit Unions should have a policy for destroying out-of-date data.

3. Credit Unions will need to ascertain if they need to appoint and train a Data Protection Officer.

4. To be secure and compliant, Credit Unions will need to integrate data protection fully into all business processes and not treat this as an add-on or side issue.
What to bring away from today – Major Items

1. Write down a set of data protection policies and procedures and ensure that these are compliant with the GDPR. Such policies and procedures should include what actions need to happen in the event of a data breach.

2. Consider what breaches might do harm to members and pay particular attention to mitigating these risks.

3. The most serious are either financial fraud or identity fraud, so Credit Unions should pay particular attention to all personal information stored on their servers.

4. Credit Unions may need to invest in education and training all employees involved in collection and processing of data with a view to reducing the risk of human error and as far as possible try and automate as many processes as possible in order to reduce the risk of human error.

5. Put in place a Cyber Crime Policy
What to bring away from today – other items

1. Are all personnel that regularly process data, familiar with GDPR and the changes it introduces to Data Protection?
2. Do you know how many personal records you process per year?
3. Do you have a process for data portability?
4. Do you have a process for data erasure?
5. Do you inform individuals about the data you process? Eg. a GDPR-compliant Privacy Notice is required.
6. Do you need to appoint a DPO?
7. Do you have a Data Protection Policy in place? You need to update it for GDPR
8. Do you have a Privacy Policy in place that can be easily found on your website?
9. Do you have sufficient data protection training in place?
10. Should you consider a data audit and setting up a data register (what, where, how and by whom data is used)
Thank you

Bernard Cogan
Client Services Director
Cuna Mutual Group Ltd
01213590221

cunamutual.co.uk/ace2017