GDPR

What does it mean to U3A?

Presented by Philip Mather and Vakis Paraskeva

GDPR Auditing Limited
in association with
U3A

In this Session

- Part 1 GDPR Quick Guide – 20 minutes.
  - What is the GDPR
  - How does it affect U3A
  - When does it start
  - Who does it affect
  - Where do I go for help
- Part 2 - Impact of GDPR on U3A – 10 minutes
- Part 3 – Lawful Basis – 10 minutes
- Part 3 – Strategies and Risks – 30 minutes
  - Strategies
  - Risks
  - Road to Compliance
- Q+A – 15-20 minutes

What is the GDPR

- The General Data Protection Regulation
- For the, UK effectively an update to the Data Protection Act 1998
- Unifies Data Protection across Europe
- Enhances the rights of European citizens in respect of their personal data
- Notable changes to the DPA are Accountability, no fees, heavier fines
- Remember: THE GDPR is Law, and not a recommendation or best practice or something that you should ignore lightly.

How does it affect U3A

- You collect, store and process the personal data for various categories of data subjects.
- GDPR is likely to be enforced more rigorously than the DPA.
- Data subjects will be much better informed about the GDPR than they ever were about the DPA
- Expectations of data subjects will be much higher and are more likely to exercise rights against less scrupulous organisations
- All parts of U3A need to take action in respect of the GDPR
- Anything else is breaking the law…….

Why Should U3A Care

- Voluntary organisation, providing activities for the good of the membership
- Older generation can be less aware of the online world and how data can be exploited (but sometimes more anxious)
- Individual U3A's have a moral and legal obligation to protect the membership
- GDPR says you must *"protect the rights and freedoms of individual data subjects"*
- Important that U3A finds ways to abide by the GDPR that are sympathetic to the volunteers and the data subjects.

When does it Start

- Hopefully U3A is already following the DPA
- If not…. for GDPR, preparation starts now
- You really should be ready by the 25th May
- But is doesn't end then …..
- Start now, do what you can before May, and keep going
- There is no cliff edge
- Brexit will not affect GDPR

Who does it Affect

- Every living person in the EU
- Controllers and Processors, both inside and outside of the EU, processing personal data of EU citizens.
- Most of you will be data controllers
  - Collectors of the data
  - Keepers of the data
  - Removing or deleting the data
  - Anything to do with the data

Where do I go for Help

- Information Commissioners Office (ICO)
- https://ico.org.uk/for-organisations/
- Ring National U3A Office
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

- Will not provide answers to every question

Impact on U3A

Impact of GDPR on U3A

- We will assume little familiarity with the DPA
- Nearly all concepts in the GDPR will be new
- The GDPR is designed to be much less ‘optional’ than the DPA
- It is about time everyone is aware of the value of their personal data and the personal data of others
- Challenges faced by U3A
  - Variety
  - Informality
  - Paper records
  - Volunteers
  - IT

Impact of GDPR on U3A

- 1000+ U3A's with the potential to be working in 1000+ different ways

- Common ground
  - Lawful basis for collecting and storing personal information
  - Informing data subjects about the, what, why where, of their personal data
  - Letting data subjects know what their rights are and how to exercise them
  - Keeping data secure
  - And removing it on request or when no longer required

THE THIRD AGE TRUST

U3A

THE UNIVERSITY OF THE THIRD AGE

Lawful Basis

GDPRAuditing

Lawful Basis – Choice?

- Consent – freely given and freely taken away, good for marketing, not so good if withdrawal of consent causes you a problem make it clear, and granular, refresh frequently
- Legitimate Interest – can be used if you don't have consent, but needs to be balanced, rights of the data subject will mostly be upheld over the controller, a bit like assuming consent
- Performance of a Contract – if you need the data to fulfil some obligation, no data = no service, all rights and freedoms can be upheld but there are usually consequences
- Important to get the right lawful basis

Lawful Basis – Logical Argument

- Where an agreement to provide a service relies on some personal data being collected then this is most likely to be ‘performance of a contract’
- Where there is no contract or implied contract and the provision of personal data is entirely voluntary then this is most likely consent
- A simple consideration is:
  - If the data subject were to request the data to be removed would there be any residual issues around notice periods, payments, data retention, or could the data subject walk away with their data as if they had never been there?
- If a single lawful basis is not obvious then it is more than likely a combination of one or more

THE THIRD AGE TRUST

U3A

THE UNIVERSITY OF THE THIRD AGE

Strategies

GDPRAuditing

Informing Data Subjects

- On your website
  - Privacy Notice
  - Cookie Policy
  - Contact forms
- Membership Application Forms
  - Online
  - Downloadable
  - Paper
- eMails
  - Newsletters
  - Other
- Event/Trip etc. sign up

Rights of Data Subjects

- Regardless of the Lawful Basis
- The data subject should be informed of the following:
  - State the lawful basis
  - Who the data controller is
  - What the data is used for
  - How long the data will be kept
  - That the subject can access the data and have it deleted, restrict or object to processing
  - Ability to withdraw consent if that is the basis
  - Right to lodge a complaint
  - Is the provision of the data necessary for a contract and what happens if not provided
  - Whether the data is likely to be passed on to a 3rd party

Exercising your Rights

- Who will be responsible for fulfilling the data subject requests?
- Do the data subjects know where to go to
- How will you:
  - Provide them access to their data
  - Remove data out of data or requested to be removed
  - Know which data you can give or not give
  - Identify a data subject well enough
  - Retrieve data sent to a 3rd party

Keeping Data Secure

- Where is it all?
- Software - Website, excel, word, database, other
- Hardware –Web server, PC, laptop, smartphone, USB, CV/DVD, tape
- How is it transmitted – email, post, social media, electronically by hand
- Who has access to it?

Removing/Deleting Data

- If your basis is only consent you will likely have to delete remove all of it
- If you have legitimate interest you will likely need to delete most of it
- If it is contractual you may have to keep some of it
- Main thing is:
  - Know what you can delete and why and where from
  - Know what you need to keep and under what basis
  - If you keep data know when you must delete it – data retention principle

Practical Steps

- Decide who in your U3A is going to be responsible for data protection
  - Chair
  - IT Guru
  - Committee
- Create an action plan to implement the requirements
- Collect data lawfully
- Secure the data you have and the data you are going to get

THE THIRD AGE TRUST

U3A

THE UNIVERSITY OF THE THIRD AGE

Risks

GDPRAuditing

7 Deadly Sins

- Where your risks are going to be
  - Incorrect or no lawful basis for collecting and storing data
  - Not identifying all categories or data subjects
  - Not informing data subjects adequately
  - Contracts or agreements with 3rd parties
  - Securing paper records, creation, storage, movement, disposal, archiving
  - Security of Electronic data
  - People – hopefully minimal

Contracts with 3rd Parties

- If the U3A sends details to a 3rd party then there will be a controller processor relationship
  - Therefore an agreement or contract needs to be in place between the U3A and 3rd party to protect the personal data
  - If no contract exists and the 3rd party suffers a data breach then the U3A would be liable
  - Where possible avoid this scenario and keep relationships between 3rd parties and members direct
- Controller, processor contracts can take time
  - Have a standard contract 3rd parties sign up to
  - Give yourself enough time
  - Use 3rd parties you trust
- 3rd Parties can be data subjects too – e.g. sole traders.

Securing Paper Records

- Likely records
  - Membership forms
  - Registers
  - Class bookings

- Actions
  - Ideally, scan and destroy (cross cut shredder)
  - Otherwise keep under lock and key - always
  - Keep an index of what you have
  - Remove/destroy old/out of date paper records regularly
  - Be prepared to handle data subject requests relating to paper records

Securing Electronic Data

- ICO unlikely to come knocking if a document isn't quite right
- But if personal data gets into the wild – that is another matter… consider
  - Bios passwords on PC and Laptops
  - Use strong passwords for logging on and change them regularly
  - Restrict access to personal data to only those that need it (shared IT) – is your device used by anyone else
  - Consider drive encryption or password protect files
  - Keep anti virus and anti malware up to date
  - Save your personal data so you cannot lose it, make sure the backup is encrypted and password protected and keep it somewhere safe – ideally another location
  - When you send personal data, send it securely

People

- Not a huge problem for U3A
  - Not large corporate machine
  - No large departments with access to data
  - Left and right arm should know what each is doing
- Actions
  - Keep personal data records between one or two individuals
  - Assign responsibility to these individuals
  - Ensure the individuals have been educated appropriately in GDPR awareness and information security (at the right level)
  - Make sure individuals know how to keep data safe, how to detect a breach and how to report it to the relevant authority (ICO)

Considering the Risk

- Proportionality – Risk – Shades of Grey
  - Quite possibly many more than 50
  - The law is black and white, implementing GDPR is not
  - Quote “implement appropriate technical and organisational measures”
  - Quote “assessment of the necessity and proportionality of the processing operations in relation to the purposes; “
- Learn how to assess information security risks
  - Why do I collect this data
  - Under what basis
  - Do I need all of it
  - How soon can I get rid of it
  - If I have to have it how do I secure it
  - What would happen if I lost it

Road to Compliance

- Know what data you hold
- Have valid reasons to hold and process it
- Make sure the data subjects know you hold it and what their rights are
- Keep data secure
- Remove any data you shouldn't have or don't need as soon as you can
- Assign a DPO to keep you in line with GDPR
- Respond to requests and breaches in a timely manner
- Ensure through contracts that 3rd party processors are on the hook for protecting your data
- Conduct risk assessments before collecting and processing new or additional data

THE THIRD AGE TRUST

U3A

THE UNIVERSITY OF THE THIRD AGE

Questions and Answers

GDPRAuditing