GDPR

General Data Protection Regulation

SALC and VCS Assembly Event
Council Chamber, Shirehall, 8th November 2017

Event Summary

Welcome

Cllr Joyce Barrow, Shropshire Council's Portfolio Holder for Communities, welcomed attendees to the event. Joyce said a few words about her porfolio, cutting across and linking to other portfolios and covering both working with town and parish councils and the voluntary and community sector. Joyce provided an introduction to the event and explained that the session was designed to:

- Enable us to learn more about the General Data Protection Regulation.
- Find out more about best practice in data protection and how to prepare for changes.
- Gain an insight into how the regulations may impact upon town and parish councils and the voluntary and community sector.
- Enable participants to will feel more prepared and able to respond to GDPR.

Joyce explained that the event was a joint event organised by Shropshire Association of Local Councils (SALC) and Shropshire VCS Assembly and offered particular thanks to Dianne Dorrell for her role in organising the session. Following important housekeeping information Joyce concluded the welcome by thanking and introducing the speaker: Rob Montgomery from Telford and Wrekin Council.

General Data Protection Regulation

Rob Montgomery from Telford and Wrekin Council presented an overview of the General Data Protection Regulation, highlighting key information town and parish councils and voluntary sector organisations need to be aware of.

A copy of the presentation slides are available. Rob has requested that these are not copied or shared with people outside of attendees own organisations.

A summary of main points is included below but more detailed guidance is available and links are provided at the end of this document.

Rob started with a quiz:
Question: 47 days to ….? Answer: Christmas.
Question: 198 days to…? Answer: GDPR implementation.

Rob explained that Data Protection willl still apply from 25th May 2018 but GDPR will modernise the Data Protection Act. GDPR is a little like adding a new roof on a house, the foundations and walls and main structures are still there but a new roof is needed or the house will start to become uninhabitable. Rob highlighted that GDPR experts don't exist yet. GDPR is a significant change and people are still working their way through the details and preparing in advance of implementation. The Information Commissioner's Office (ICO) builds on cases taken to court so some areas will not have been investigated and explored in the court arena.

Rob explained that, with Local Authorities providing hundreds of services, there is a good chance that things will go wrong occassionally and, although town and parish council's and voluntary sector organisations have a reduced chance of making mistakes, mistakes can happen and it is important to manage that risk and deal with issues effectively when thety occur.

Rob spoke about the outdated Data Protection Act 1998. Advances in technology after that time mean that data is being collected and stored in new ways. One example is use of the Cloud. Security of systems is a big area of focus under GDPR.

Fines for a data breach are significant. The maximum penalty currently permitted under the Data Protection act is £500,000. However, under the the General Data Protection Regulation, which will come into force in May 2018, the penalties for a data breach will either be €20m (£17m) or 4 per cent of annual turnover.

Individuals can request copies of all information an organisation holds about them and that information has to be provided within 40 calendar days.

Rob provided more information about the regulation.

- The UK is committed to implementation and GDPR will feature in UK legislation despite Brexit.
- 99 articles and sub clauses
- 173 recitals (supplimentary articles)
- UK derogations – we can decide certain elements for the UK (one example is that a child will be able to consent to their data being used at age 13 in the UK and in the EU GDPR regulations it is 16).
- The changes only relate to personal data.
- Under GDPR sensitive personal data is now called special category (e.g. ethnic group, sexual orientation etc)
- There are now 6 principles and there were 8 under Data Protection.

Rob warned against data breaches using examples such as:

- Leaving notebooks and laptops in public places or in car (a locked boot is OK on a temporary basis to travel).
- Sending an email containing personal data to the wrong person.
- Sending a letter to the wrong house.
- Incorrectly disposing of data (e.g. using a public bin).

Under GDPR all data breaches must be reported to the Information Commissioner's Office (ICO). This is a change from current legislation. There are 72 hours in which to report to the ICO. Fines could be €10 million for not reporting. Breaches a where an individual's rights and freedoms have been affected. The individual must be told. Information to report includes type of breach, number of people affected, mitigating actions taken.

Robs advice on things to consider included:

- Ensuring the organisation has a coodrinator responsible for GDPR. Clarifying responsibilities of staff.
- Putting in place a data breach procedure for all employees, contractors, volunteers etc.
- Understanding the need to act quickly within the 72 hours timeframe (having a process to follow).
- Easily accessible information on where to report, how etc.
- Clear lines of responsibility – decision taken by Board etc.
- Putting in place encryption.
- Only collecting information really need.
- Checking addresses.
- Using initials or other ways to ensure an individual is not identifiable.
- Ensuring people are trained.
- Having robust policies and procedures in place to cover GDPR.
- Implementing privacy notices (e.g. as part of forms).
- Having a retention policy and implementing retention periods for data.
- Being clear on the legal reaon for processing the information.

- Having information available on websites so people see the organisation is committed to GDPR and how it uses data and keeps personal data secure.

GDPR also brings changes to processing requests for data. Organisations can currently charge £10 to process a request but there will be no chanrge under GDPR and the time to process has also reduced in the regulations from 40 days to 1 month. There are still some exemptions.

Rob highlighted some key elements:

- **Rectification** – People can request changes to their data – need to ensure IT systems will allow that. Can not dispute opinion however. If you have shared data with another organisation they will have to be informed and changes made.
- **Right to be Forgotten** – Under GDPR there is a right to be forgotten and all data relating to a person must be deleted unless there is a legal reason to keep it. If data has been shared with anyothr organisation they would need to delete too.
- **Ristrict Processesing** – An individual can request that a stop/hold is placed on data processing while you discuss their concerns or agree a way forward.
- **Data Portability** – An individual can request that the data you hold on them is converted into a portable format (e.g. csv) and transferred to another organisation (for example someone moving schools).
- **Object to processing** – For example you can onject to cld calling.
- **Automated decisions** – You can request that your data is handled by a person rather than an automatic process within a system.

Key points to consider highlighted by Rob included:

- Right of access – check systems and IT to ensure you can respond.
- Consent – check whether this applies. Consent is implied within a contract – e.g. you have to provide information in order to receive the service/product you have asked for.
- Double check that you are not using pre-ticked boxes forconsent – that is not allowed under GDPR – consent is not opt out – it has to be clearly given as a positive action and silence is not a form of consent.
- Sensitive data can be kept under 2 legal reasons and consent is one of them.
- You must be clear how someone can revoke consent.
- Consent is for a specific reason.
- You must record how consent was given and what it was for.
- You cannot refuse a service because someone did not give consent.

Accountability was another key theme of the presentation. Rob explained that all organisations must demonstrate that they are complying with GDPR.

- Technical elements of this compliance can include passwords, encryption, user IDs, etc.
- An information asset register should be kept.
- Privacy by design - Data protection impact assessments should be completed.
- Minimise personal data recorded.
- Make personal data non identifyable where possible.
- Be clear what the data is used for.
- Risk assess and put in place the right tools and procedures to manage that risk.

A Data Protection Officer must be appointed for the organisation but Rob explained that that person could be for a group of parishes or organisations if that was easier. Rob spoke about Telford & Wrekins offer and this offer with costs is available as a separate document. The DPO should:

- Advise the organisation of responsibilities
- Report to the highest level in the organisation
- Cannot be dismissed
- Must have knowledge of the law/GDPR (should have training).

Questions and Answers
There were a number of questions and some of the key points from the answers are sumarised below:

- Previously if you contracted with someone to deliver a service for you you retained responsibility but this changes under GDPR. The company responsible for a data breach is at fault.
- The ICO will issue guidance for small organisations.
- Undertake risk assessment for data – if there is a very small risk of breaches, if little personal data is collected/volumes etc. then the organisation will not need to invest as much in meeting requirements (but should have the basic elements and procedures in place as good practice).
- If funders require the collection of sensitive data the funder should give the legal reason why that data should be collected (challenge when necessary).
- The Equalities Act could be a reason to collect some data.
- Some data will be collected for a contract and so consent isn't needed. For example a village hall booking or booking community transport. Even if don't need consent it is good practice to set out what data is being collected, how and why. Transparency is important.
- Councillors may be using their own private emails to communicate but any activity carried out for the organisation/ business matters must be disclosed.
- For under 13s parents can give consent. If 13 or over and they have capacity a child can consent and should know and understand what is happening with their data.
- Targetting online services at children is a big area of concern nationally and something to be aware of.
- Records management retention is an important area to consider.

Important Links
European website for GDPR
http://www.eugdpr.org/

Information Commissioner's Office GDRP guidance
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

NALC Letter
http://www.nalc.gov.uk/library/news-stories/2539-data-protection-bill/file

NCVO website and resources
https://www.ncvo.org.uk/practical-support/information/data-protection?highlight=WyJnZHByIl0=