Briefing Paper: General Data Protection Regulation

With less than 100 days to go the SCSN staff team have been thinking about the General Data Protection Regulation (GDPR) and what it means for us and wanted to share with you some of our preparations for it coming into force. We also thought we'd have a think about the implications for those working within our partner organisations and in the partnership context. This briefing paper is based on an article in our April 2018 newsletter.

We know that the introduction of new legislation can cause concern and confusion. Sometimes organisations can become more risk averse in this climate and can limit information sharing between partners and stifle new processes seeking to develop data sharing. We believe that sharing information should and always will be an essential part of partnership working. It has a key role to play in improving public services and keeping people safe, so we want public sector organisations to be clued up on the GDPR so they are confident in sharing information.

The changes which the GDPR bring, are predominately about firming up your data management practices (i.e. recording things more and bettering how you record them, improving the content of your privacy notices, and the way you ask people for consent), rather than a total overhaul of your systems and processes and a change in approach to information sharing within partnerships.

PART I BACKGROUND

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018. GDPR is an important piece of legislation designed to replace existing data protection rules with a new framework which accounts for recent technological advancements. It will effectively replace all data protection legislation across the EU - including the UK's Data Protection Act (DPA).

GDPR will significantly raise the bar of obligation and accountability, ensuring that all organisations which handle personal data adhere to strict regulations around privacy, security and consent. It aims to reinforce data protection regulation for new technologies, while allowing people to have more control over their data and feel their personal information is safe. The Information Commissioner's Office (ICO) have a dedicated section of their website to the GDPR which we would recommend looking at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

This isn't the full story however: the UK government has published its draft Data Protection Bill (DPB), which will in effect implement the GDPR and give provision for some of the exemptions such as the Law Enforcement directive. It hopes to provide continuity during and after Brexit and to 'Brexit proof' the legislation so that it continues to work in a post-Brexit environment.

The advice is that the DP Bill and the GDPR should be read side by side, and that organisations should continue preparing for GDPR.

IN BRIEF

The GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from.
This means that people handling and sharing personal information because it is necessary, proportionate and appropriate and carried out in a secure way can continue to do so; but there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently. Some examples of things that will need to be done differently are listed below (1 and 2) and some things which will need to be done for the first time (3 and 4). This list is not exhaustive so looking through some of the further reading links or asking your Data Protection Officer for how it affects you, your organisation and the partnership is important.

1. For example the GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

2. All information held on subjects under the age of 13 must have parental consent (unless there is another legal basis for collecting the information, for example under the law enforcement directive).

FURTHER READING

Read more about the UK Bill here:

https://ico.org.uk/for-organisations/data-protection-bill/

https://united-kingdom.taylorwessing.com/en/insights/radar/uk-data-protection-bill-published

http://www.computerweekly.com/feature/UK-Data-Protection-Bill-vs-EU-General-Data-Protection-Regulation.

And to read the Bill in full
https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066.pdf.

For detailed factsheets and guidance for various types of organisations the Information Commissioner's Office (ICO) has a great page
https://ico.org.uk/for-organisations/
They have pages on charities, small organisations (the ones to which we have referred whilst preparing for our obligations, law enforcement and justice bodies and local government.

There are factsheets on the UK DP Bill sections which are most relevant to CSPs and their partners here:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644826/2017-09-13_Factsheet03_law_enforcement.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644634/2017-09-13_Factsheet01_Bill_overview.pdf

3. For example GDPR puts provisions in place for higher fines and new timescales on reporting a breach (72 hours). So from a purely financial perspective, the potential consequences of GDPR noncompliance are significantly greater than under the old regime. Information about sanctions imposed will also be in the public domain - so possible reputational risks to the organisation also need to be considered. Organisations will need a clear protocol in place in the event of a breach.

4. For example new provisions around consent. You are not required to automatically 'repaper' or refresh all existing Data Protection Act (DPA) consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. Data subjects must be issued 'privacy notices' and statements on the purpose of the data collected. Third parties with access to information must now be explicitly named.

    a. This applies to us here at SCSN in relation to our member and mailing list's contact details and our personnel files but is less relevant to personal information CSPs might share between partners as the lawful basis for sharing information is different i.e. prevention and detection of crime or personal or public security for example. This issue will apply to CSPs for information voluntarily given for referral to a particular service then being used/kept on an additional vulnerability database for example. CSPs should consider this issue very carefully.

5. For example many of the rights of individuals are the same under GDPR as they are under current DP legislation, but the data subjects now have strengthened rights including the right to change or delete their information. The right to data portability is new. It only applies:

    a. to personal data an individual has provided to a controller
    b. where the processing is based on the individual's consent or for the performance of a contract; and
    c. when processing is carried out by automated means.

    Under this portability aspect you should consider whether you need to revise your procedures and make any changes.

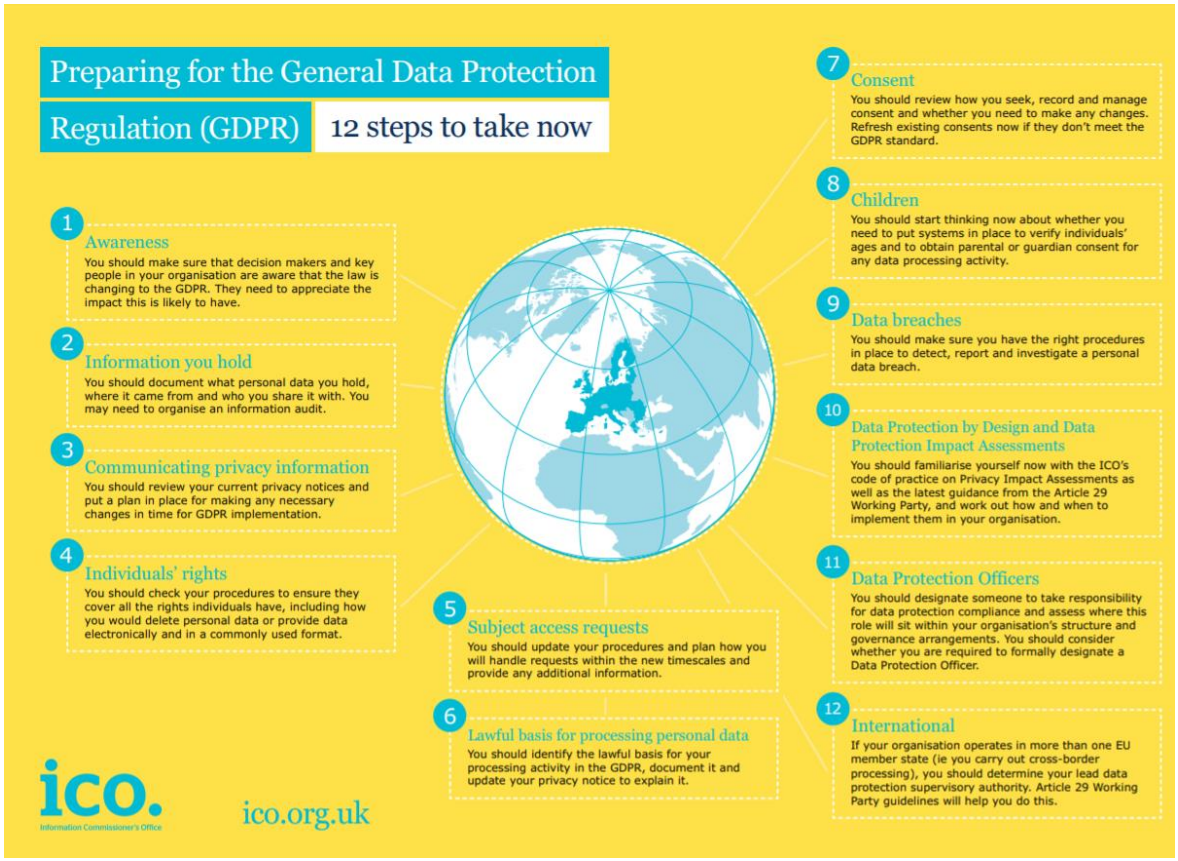
    If asked for what information you hold on an individual you will need to provide the personal data in a structured commonly used and machine readable form and provide the information free of charge and within 30 days (new timescale). This is unlikely to apply to SCSN (we don't carry out processing by automated means) but could apply to CSPs where the processing is made on the basis of consent (for example voluntary referral to a youth work service or home safety visit service) or the processing is carried out automatically (this applies to any database for example of criminal

records). The issue of consent as a legal basis for processing information (see point 3) and information only being used for the purpose for which it was given comes into play here.

So now we're all ready for 25th May!

If the answer is no or even um, maybe…the ICO has created a section on its website which gives guidance to organisations getting ready for the GDPR one of which is shown below. At SCSN we found this a helpful place to start our preparations. Visit here https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ for more information.

PART II GETTING READY FOR THE GDPR



In brief, to be compliant all organisations should create a compliance audit and action plan including the following tasks:

1. Appoint a data protection officer (DPO) or have a member of senior leadership team act as an ambassador
2. Establish a system that documents all data processing activities (a data audit)
3. Do 'compliance assessments' on all policies and procedures

4. Review contracts and terms and conditions to include 'enhanced responsibilities'
5. Review the technical and organisational measures that need to be put in place

Being open and publishing these plans and activities is an important step in transparency and accountability – we at SCSN have done this in our April 2018 newsletter article and will be publishing more as we near and pass the compliance date in May.

Some considerations for CSPs at this stage would be:

- **Think about what data you hold, how is it kept safe**
  - Especially if there are things like cloud storage, encrypted devices, working from home, physical movement of paper-based information and separate excel 'databases' containing personal information)

- **Think about what you use the data for, how you share it. Do Information Sharing Protocols (ISPs) require updating in light of GDPR?**
  - There will be issues and implications relating to (but not limited to) the lawful basis for gathering the information which will impact what you can do with the information e.g. sharing with third parties or information sharing between partners and for what purpose.

- **Do you have in place breach protocols? Do these fit in with the new timescales (72 hours) stipulated in the new regulations?**

- CSPs hold and share personal information in relation to children – **under GDPR this will need closer examination due to the additional safeguards in place**

- **Think about awareness of the new regulations**
  - Are all partners aware of the new regulations?
  - Do they know who the designated data protection officer (DPO) is?
  - There could be merit in each of the partner's DPOs meeting to discuss the implications of GDPR on the partnership

- **Think about whether privacy impact assessments will be needed** for any aspect of the CSP's work.

WHAT HAS SCSN DONE?

We have ensured staff awareness of the new regulations and whilst we do not require a data protection officer we have appointed a member of staff as a lead for data protection issues and appointed a Board member as an ambassador to support the work.

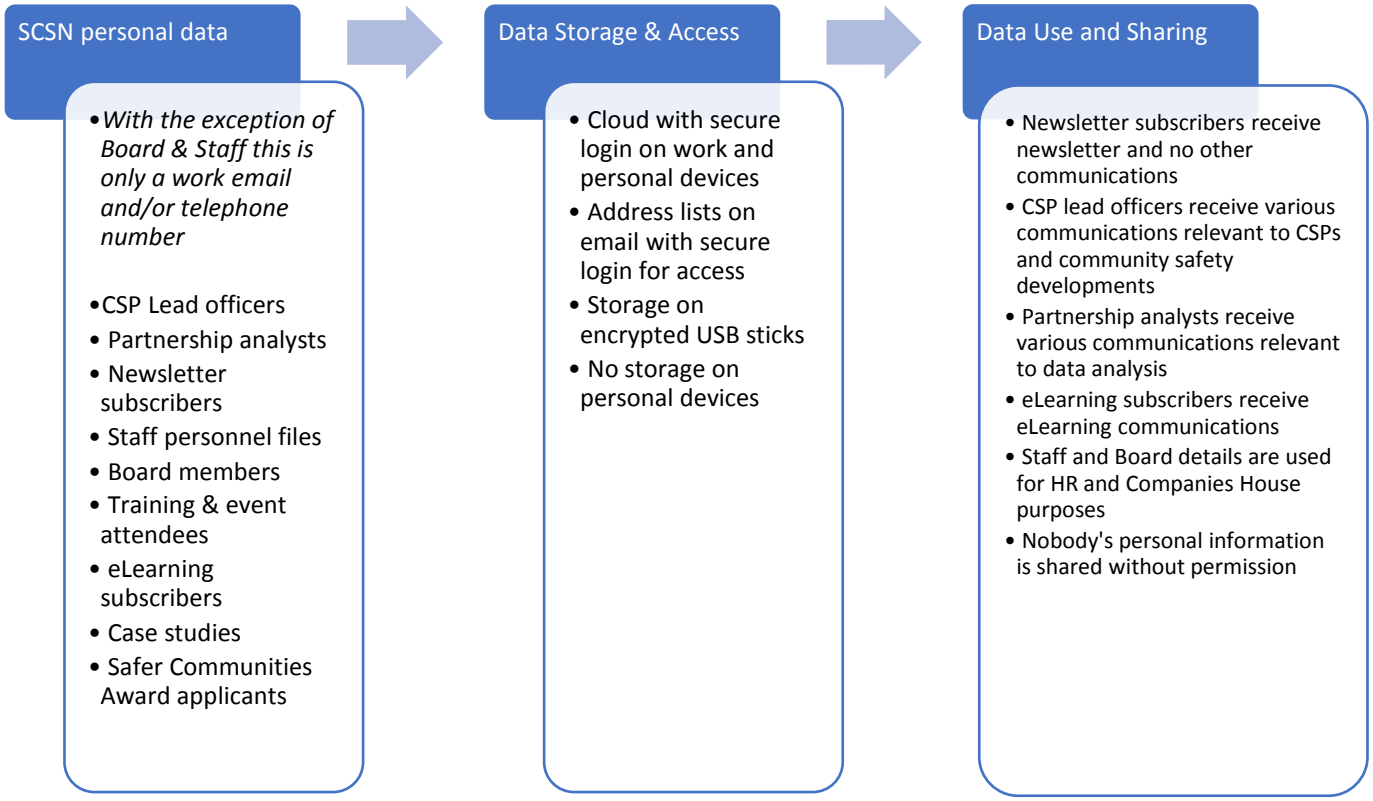
We have considered all the personal information we hold and how we store, access and use it and will be undertaking a full data audit.

We are in the process of reviewing our policies and procedures in relation to personal information and will be updating them to ensure compliance with GDPR. We will share all of this in due course.

- For example, in changes to daily tasking or multi-agency meetings or the evidence-based strategic planning or early and effective intervention process.

So What Does This Look Like in Practise for SCSN?

✓ We have completed the checklist compiled by the ICO as data processors https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/. Partnerships should consider doing the same.



✓ A particular consideration for us has been the move to more agile working (working from home and other locations, working whilst travelling), accessing information on a Cloud and using personal devices such as laptops and phones. We have given a lot of thought to what we need to put in place in order to protect the personal information we hold.

✓ We will go through our existing policies to ensure it stands up to the new GDPR. This may result in new policies, procedures and protocols and may require us to contact data subjects directly as we work through this process. We will publish our new policy once this work is complete.

So what should partnerships be doing?

This paper is not giving the 'right' answer to partnerships. There are specific exemptions within the GDPR which are covered by the UK DP Bill, specifically law enforcement. This is very relevant to CSPs. The exemption allows other organisations to disclose information to the police and similar bodies when it is necessary to prevent and detect crime. https://ico.org.uk/for-organisations/police-justice/ has a lot of great guidance in relation to law enforcement and GDPR.

However here are some specific things that partnerships should begin to think about:

- **What personal information does the partnership hold? How is this information stored, accessed and shared? How is it deleted?**
  - Does the partnership need to re-contact data subjects under the new regulations?
  - Does the partnership need to create new privacy notices when recording personal information once GDPR comes into force?
  - Review the partnership ISP in line with GDPR – does it require any amendments or to be rewritten?
  - How long can the partnership hold this information for?
  - What is the legal basis for recording and sharing personal information? i.e. is it consent-based or based on other legal basis for example prevention and detection of crime, protection of life. Information that is collected and shared based on perceived 'vulnerability, risk or harm' will require careful consideration.

All of this is particularly important in relation to information taken from IT systems and stored on an excel spreadsheet e.g. a vulnerable persons database, incident spreadsheets used by partnership analysts. Think carefully about whether information is stored on encrypted USBs, when information is stored on clouds, information on paper etc.

- **Do protocols and policies need to be updated?**
  - Is there a protocol in place for any breaches?
  - Does it meet the new timescales and requirements?
  - Are you able to provide information to data subjects and members of the public in relation to data portability?

SCOTTISH GDPR READINESS PROJECT

Specific to Scotland, the 'Scottish Digital Office GDPR Readiness Project' has allowed local authorities to work together to produce resources which have been shared amongst 30 councils. A helpful article can be found at

http://futurescot.com/local-government-scotland-gdpr/.

For those working within Local Authorities contact your Data Protection Officer for more information.

- Does the partnership ISP need to be updated in line with GDPR and the UK DP Bill?

This list is not exhaustive but lists some things we think CSPs should consider. All partners will have a DPO who can assist you with specific questions and the ICO will also be able to answer specific questions.

PART III THE FUTURE

We (SCSN) have some work to do in relation to opt in consent for our various contact lists, privacy impact assessments and data protection by design; and in relation to our eLearning terms and conditions. We also have some work to do to review and update our existing policies governing personal information.

As we seek to expand our capacity, influence and reach, possibly gathering more personal information on the way, the point about "data protection by design" will become increasingly important for SCSN to consider. Watch this space as we work through what the new regulations mean for us, we will be keeping you updated on what we are doing and anything that affects what you should be doing! Get in touch if there is anything you want to ask us about this on Twitter @SCSN2 or via email dawn.exley@scsn.org.uk.