DISCUSSION

RIBBLE VALLEY BOROUGH COUNCIL
REPORT TO ACCOUNTS AND AUDIT COMMITTEE

Agenda Item No 8

meeting date: 11 APRIL 2018
title: GENERAL DATA PROTECTION REGULATION (GDPR)
submitted by: DIRECTOR OF RESOURCES
principal author: LAWSON ODDIE

1 PURPOSE

1.1 To provide members with details of the new requirements under GDPR for discussion.

1.2 Relevance to the Council's ambitions and priorities:

- Community Objectives – none identified
- Corporate Priorities - to continue to be a well-managed Council providing efficient services based on identified customer need.
- Other Considerations – none identified.

2 BACKGROUND

2.1 Currently, all organisations in the UK that collect, process or store personal information must comply with the Data Protection Act 1998 (DPA), or face fines of up to £500,000 in the event of a data breach.

2.2 The DPA will soon be superseded by the EU General Data Protection Regulation (GDPR), which introduces tougher fines for non-compliance and breaches, and gives people more say over what companies can do with their data. It also makes data protection rules more or less identical throughout the EU.

2.3 The EU's General Data Protection Regulation (GDPR) is the result of four years of work by the EU to bring data protection legislation into line with new, previously unforeseen ways that data is now used.

2.4 The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

3 REQUIREMENTS AND RIGHTS UNDER GDPR

3.1 Like the Data Protection Act, GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and expansive providing a wide range of personal identifiers that constitute personal data, reflecting the changes in technology and the way organisations collect information about people. Attached at Annex 1 is a useful guide.

3.2 It can be assumed that any data held that falls within the scope of the Data Protection Act will also fall within the scope of GDPR. It not only applies to electronic personal data but to manual filing systems.

3.3 The data protection principles under GDPR set out the main responsibilities for organisations. The principles are similar to the current DPA principles (fair and lawful, purpose, adequacy, retention, right, security, international), with added detail at certain points and a new accountability requirement.

3.4 The accountability principle requires that the organisation put in place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

3.5 The following procedures, policies and frameworks will become a requirement under GDPR and should minimise the risk of breaches and uphold the protection of personal data:

- Information Audit
- Establish an information asset register
- Privacy Impact Assessments
- Documented procedures for Subject Access Request
- Privacy by design

3.6 GDPR also creates some new rights for individuals and strengthens some that currently exist under the Data Protection Act.

- 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

3.7 A duty is placed on all organisations to report a data breach to the Information Commissioner's Officer (ICO) within 72 hours of the organisation becoming aware of it and to inform affected subjects as soon as possible.

3.8 The ICO will be supervisory authority for the UK. Under GDPR the ICO will have the power to spot audit organisations with little prior notice. If the ICO find that an organisation is not compliant to GDPR they have the power to fine and/or stop the organisation from processing personal data

3.9 Under the Data Protection Act the ICO could apply fines of up to £500,000. Under GDPR lesser incidents could expect fines of up to £7.9 million or 2 per cent of the organisations global turnover (whichever is greater). More serious violations could result in fines of up to £16 million or 4 per cent of turnover (whichever is greater).

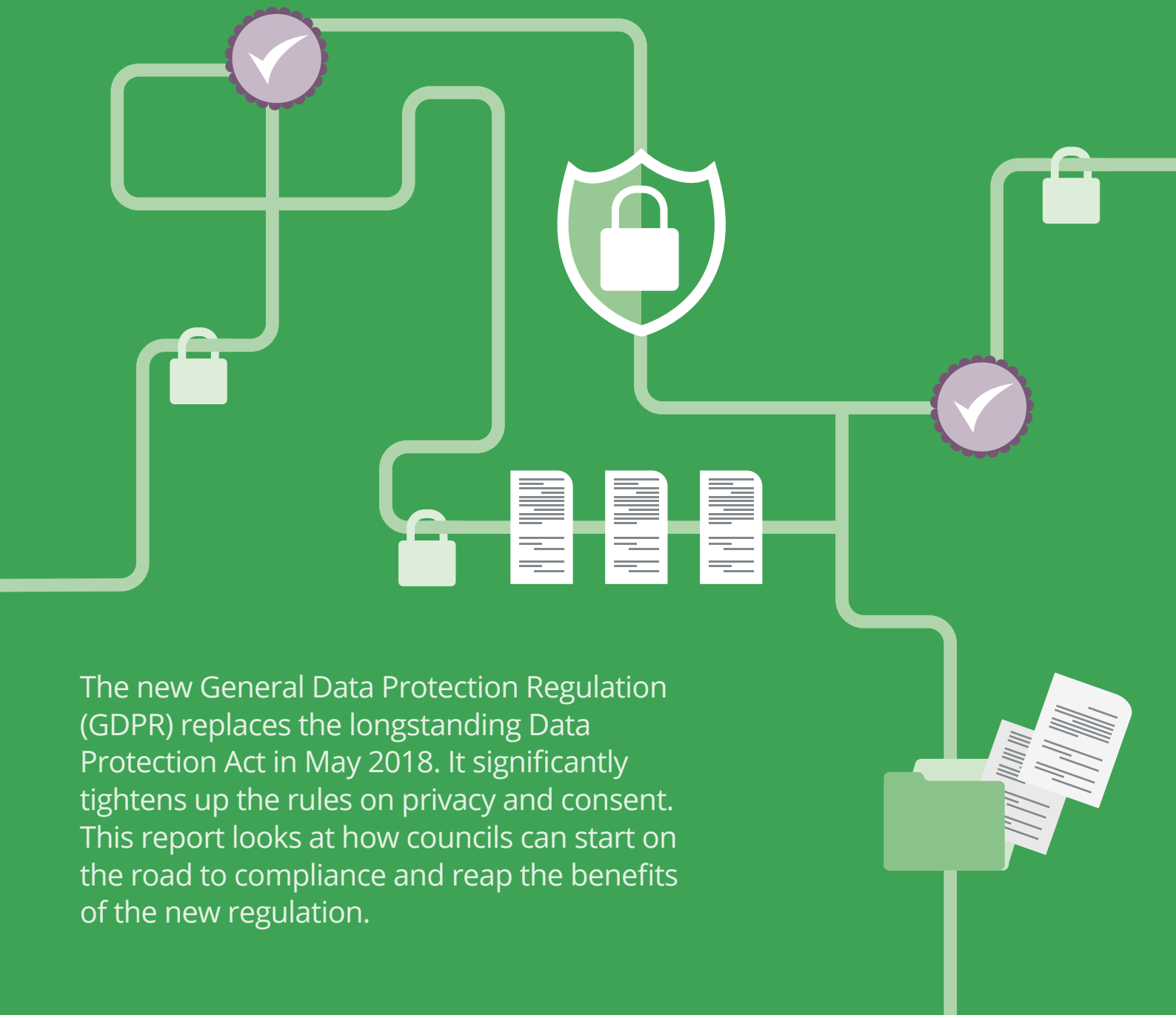
4 CONCLUSION

4.1 The new GDPR requirements will apply in the UK from 25 May 2018.

4.2 There is a high level of workload in the short to medium term to ensure that we are compliant with the new requirements. It is possible that this high level of workload **may** continue longer term under GDPR.

HEAD OF FINANCIAL SERVICES DIRECTOR OF RESOURCES
AA8-18/LO/AC
3 April 2018

Guide to GDPR for Local Government



The new General Data Protection Regulation (GDPR) replaces the longstanding Data Protection Act in May 2018. It significantly tightens up the rules on privacy and consent. This report looks at how councils can start on the road to compliance and reap the benefits of the new regulation.

eduserv
IT for public good

Why the time to take action is now

The new General Data Protection Regulation increases individuals' rights on personal data and will be fully enforceable by May 2018.

The implications for councils are widespread. Soon, all UK public sector organisations will need to have consent or one of five other specific legitimate reasons to hold and process individuals' data, including all legacy data. GDPR also stipulates the right of citizens:

- to be forgotten
- to make subject access requests at any time
- to have their data protected by processes of encryption or pseudonymisation
- to prevent direct marketing
- to prevent automated decision-making and profiling, and
- to obtain and reuse any data held.

It's worth noting that these obligations are applicable to both data controllers and processors.

Time is now short. Among many other challenges, councils are facing a huge task auditing legacy data to find out where it all is and identify whether consent was granted correctly. They also need to delete records where it wasn't or where new consent can't be obtained. These are time consuming processes. Going forward, local authorities will also need to ensure that privacy is designed into processes and services by default. Overall, this could significantly change the way councils want use personal data as part of the way they manage, analyse and deliver local services in the future.

However, this should not be seen as a bad thing.

In fact, councils should take the opposite view, because the changes that will need to be made will ultimately prove to be positive. GDPR, if implemented correctly and in the right spirit, will help councils to foster the public's trust in the way they work.

In the following pages, we explain how.

> Sound, well-formulated and properly enforced data protection safeguards help mitigate risks and inspire public trust and confidence in how their information is handled by businesses, third sector organisations, the state and public service.
>
> Information Commissioner's Office

The GDPR to-do list

GDPR compliance can at first seem daunting, but it becomes a lot easier with a clear view of what needs to be done and why. While this list is not exhaustive, these are the key areas that councils need to prioritise:

✔ Dealing with consent

One of the most pressing task for councils is the need to deal with the issue of consent. The regulation stipulates that anyone councils hold information on must give their explicit and 'informed' consent for their data to be retained for a set period of time and processed, which means the individual must be made aware of how their information is protected, what it's used for, and what the risks are.

There are a number of other hurdles to leap, because:

- this doesn't just apply to current or future data, which means councils are going to have to carry out a hefty data cleansing and consolidation programme.
- GDPR states that consent has to be specific, informed, unambiguous and freely given, which means that individuals cannot be chased or unduly pressed for their consent (councils will need to apply much rigour to this process, because records also need to be kept to evidence that consents have been properly secured).
- they also need to consider the position of minors, because children under the age of 16 cannot give consent
- there are issues with 'sensitive personal data', which includes data revealing racial or ethnic origin, political opinions and so on. Councils, like any other organisation, will need explicit and specific consent for the exact purpose or purposes for which any of this sensitive personal data will be used.

Recommended action

It's clear that the issue of consent is the most labour intensive element of GDPR. As such, it should be your starting point.

✔ New privacy policy agreements

GDPR makes organisations responsible for giving people clear and adequate information about how their information will be protected. This means most will need to develop a new, much more user friendly Privacy Policy Agreement that is written in plain English.

Recommended action

Engage a combination of legal, digital and content expertise to ensure you deliver a policy in a format and language that is clear and compliant.

✔ Subject access requests

GDPR gives individuals the right to make a subject access request at any time and get a response within one month. There's a big incentive to get this right, because it will make data management processes more efficient. If councils don't get this right, however, there is risk of considerable financial penalty.

Recommended action:

Look at ways to make the process efficient through automation or self-service (see page 9).

✔ The right to be forgotten

Under GDPR people have more power to withdraw their consent and get their data amended or deleted. In other words, they have the 'right to be forgotten'.

Recommended action

If you have cleansed and consolidated your data in order to manage consent better, this task will be easier. Councils should check as soon as possible whether the IT systems they use will actually allow the right to be forgotten to happen. Many systems don't, even some from leading vendors. If this is the case, councils should put pressure on their IT providers to include a 'right to be forgotten' facility in future upgrades.

✔ Pseudonymisation and anonymisation of data

When councils are going through their data cleansing process, they will find that some of those records can't be deleted even if the subject has asked to 'be forgotten'. This might be for reasons of financial regulatory compliance, or for a number of other reasons where organisations can show they have 'legitimate' reason for retaining and processing the data. GDPR recommends that you will need to pseudonymise or anonymise the data you can't legitimately delete to be compliant.

Recommended action:

Pseudonymisation and anonymisation are time consuming, specialised processes. Many councils will probably need new systems or external help to carry them out.

✔ Appointing a DPO

GDPR will require councils to appoint a Data Protection Officer (DPO) to achieve compliance. GDPR specifies that DPOs are responsible for activities including monitoring compliance, educating staff on their responsibilities, providing advice on privacy impact assessments and co-operating wherever necessary with the relevant supervisory authority.

Recommended action

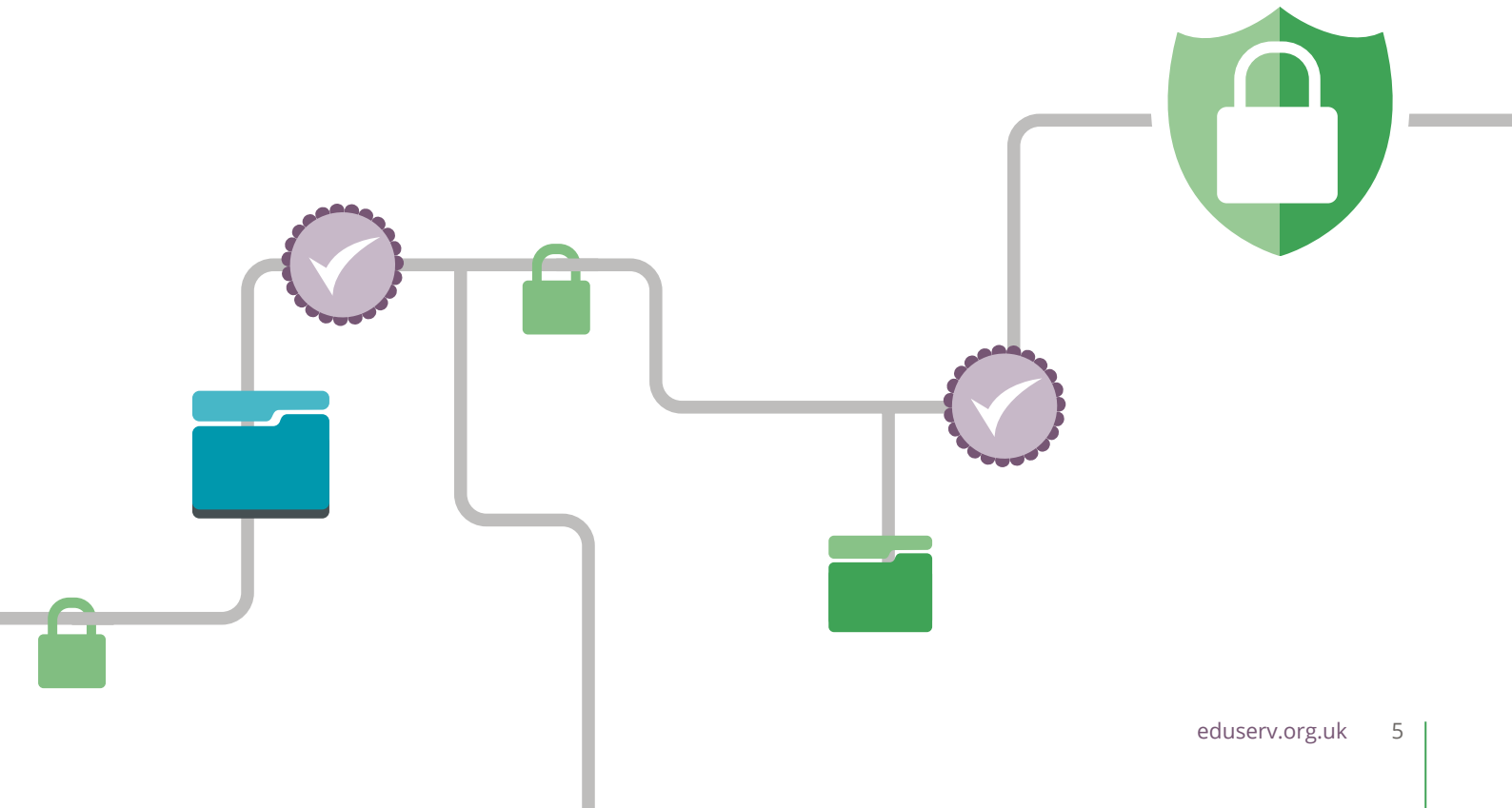
Although it is not a requirement, councils should check if potential DPOs are cyber security aware and trained. GDPR compliance implies implementing Cyber Security Regulations, so your DPO will need to be up to speed with the latest thinking on cyber security and broader organisational resilience. If they are, they will help to guarantee your data's security, integrity and accessibility by disseminating cyber security best practice throughout your organisation.

✔ Reviewing relationships with suppliers

It's not on many people's radar yet, but GDPR is also going affect councils' relationships with IT suppliers. This is because by enhancing the rights of data subjects, GDPR not only increases the responsibilities for data 'controllers' (i.e. your organisation), but also for data processors (i.e. your IT service provider or cloud provider).

Recommended action

Under GDPR, both controllers and processors are under a similar duty to ensure that the regulations are properly implemented. Contracts will need to be reviewed so that both parties comply with the regulations.



Timeline

What do you need to do and when? A phased approach that prioritises the heavy lifting first will help you achieve compliance effectively.

1 Raise awareness of GDPR among leadership and get their support

Be positive and explain the business benefits of GDPR to get full backing for your programme.

2 Identify and map processes that involve personal data

Audit all your personal data to find out where it is, where consent was granted, technical measures for ensuring its security and who controls it (you or a third party).

Also assess existing organisational processes (or lack of them) for data protection, including scenario based exercises, security and vulnerability testing.

3 Understand the legal grounds on which you currently collect and use data

In particular, examine how consent and 'legitimate' interests are used as the basis for processing personal data and document these. Where it's not obvious, contact the ICO for clarification.

4 Review skills and start recruitment of your DPO

Make sure you carry this out early, because people with the relevant skills and DPOs with the right knowledge of local government are going to be in short supply in the run up to May 2018.

5 Prioritise your plan of action

Once you know what data you have and the condition it's in, it's time to focus on building the systems and processes you're going to implement. Key areas include:

- cleansing and consolidation of legacy data
- pseudonymisation and anonymisation of data you are legally obliged to retain
- subject access requests
- the right to be forgotten
- privacy by design for collection of all future data.

6 Review relationships with your IT suppliers

Assess how your working relationship will change and review and redraft contracts where necessary.

7 Check the current IT systems you use are up to the job

Assess whether your IT systems will work under GDPR – some, for example, currently make it very difficult to implement the right to be forgotten.

8 Review and update privacy policies

Rework all privacy policy statements to ensure they are in plain English and present a friendly face to the public.

9 Update leadership and the rest of the organisation

Celebrate success and reinforce the business benefits your organisation is likely to achieve as a result of GDPR. Remind everyone that they share equal responsibility for data protection in their day to day roles.

10 Implement processes

In the run up the compliance deadline, ensure any new processes (and education programmes) you are implementing are embedded as business usual.

Opportunities to improve practice

As well as improving data protection and fundraising practice, there are opportunities under GDPR for councils to improve the way they operate.

Cyber security and resilience

James Mulhern, Chief Information Security Officer for Eduserv.

Right now, councils are being threatened by cyber-attacks and data theft more than ever before.

This is especially true in areas of council work that involve social care or any area where they might need to gather 'sensitive' data covering health, sexual orientation, race, gender and so on. Indeed, evidence gathered via the dark web suggests that personal information like this – such as a stolen care record – is now more valuable for cyber criminals than financial information like credit card details.

Reducing your attack surface

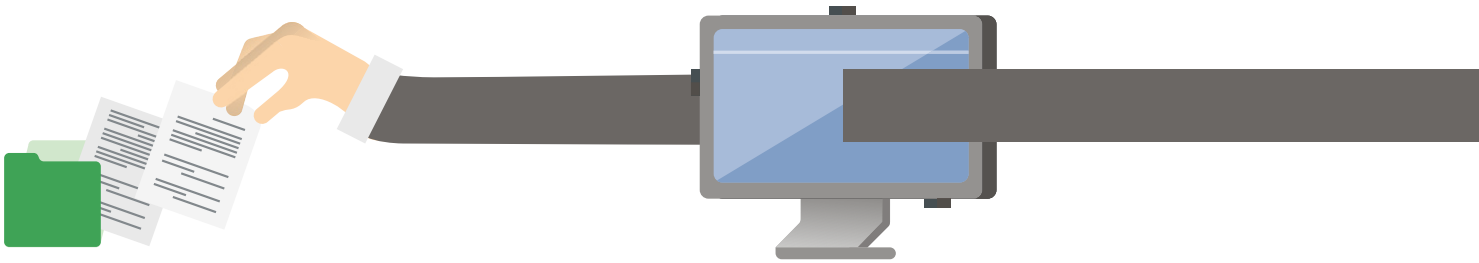
This is why GDPR is a good thing. If you're responsible for cyber security, GDPR is actually a golden opportunity to get a firmer grip on this key area where attacks are increasing.
For a start, the process of retrospectively cleansing, pseudonymising or anonymising data that is key to GDPR compliance provides an opportunity to reduce the value and sensitivity of data currently exposed to cyber criminals. Put simply, you can use GDPR to reduce your overall 'attack surface'.

Improving organisational resilience

Of course, we should also recognise that organisational and human factors are just as important as any technical barriers you put in place to prevent attack. The General Data Protection Regulation confirms this, stating that in order to achieve compliance, organisations are going to need to demonstrate that they have robust processes in place for regularly testing, assessing and evaluating the effectiveness of not only technical measures but also the organisational measures for ensuring 'security'.

That means they'll need to think about providing security and GDPR awareness sessions that improve understanding of personal and sensitive data across the organisation. In addition, they should consider performing security incident response planning, red teaming and advanced resilience testing, based on both covert and overt scenarios.

These activities should not be seen as a burden. Rather, they should be seen as the opportunity to introduce best practice that many organisations – especially those who hold really sensitive data – should have introduced years ago.



Digital services, websites and apps

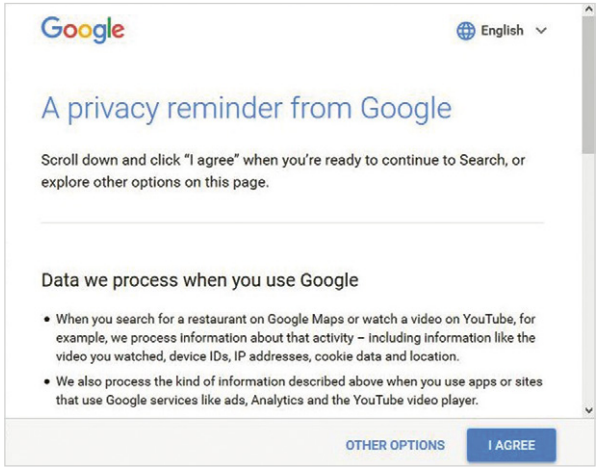
Vee Rogacheva, User Experience (UX) Designer for Eduserv.

On the face of it, GDPR's more stringent requirements for gathering personal data appear to have the potential to make digital services much clunkier to develop and engage with.

I take the opposite view. Digital leads in councils should in fact be looking at GDPR as a way to improve the user experience. Take the way Privacy Policies are handled and the requirement to use plain English. There are some great examples out there already of how the tone of voice is changing.

Organisations that are already using GDPR to improve user experience

Major data-gathering organisations like Google and media outlets like the Guardian, have recently take a lead on this by developing new privacy policy pages and content (a video, in the case of The Guardian) that present a much friendlier and transparent face to their organisations. Digital departments in councils that want to inspire public trust in digital services are looking for inspiration or guidance when they come to revamp their own policies would be well advised to look at these as examples of very good practice.



Google's new privacy policy presents a friendly welcome to users that want to learn more

Digital can also help new GDPR related processes run smoothly

There are many other ways that digital can help GDPR compliance to run smoothly and boost efficiency. Consider Subject access requests, for example, which gives users the right to check the data you hold on them and what you do with it at any time.

The danger is that this process, if handled badly, could become very laborious for both the users making the requests and the organisations that need to respond to them. However, digital specialists have an opportunity to make a difference here by following one of the GDPR's key best practice recommendations. This states that organisations should try to provide a secure online self-service system that provides the individual with direct access to his or her information.

This kind of 'Manage your privacy settings' system is only a recommendation and not compulsory, but it could be well worth exploring if your council is committed to digital transformation. In effect it could be a new digital service that organisations can develop to streamline potentially time consuming processes. It will also provide a better user experience. Getting there will require investment and technical development, but the incentive is that over time this kind of service could become a clear demonstration of your council's overall commitment to transparency and creating trust in online public services.

The main job for digital departments with regard to GDPR will be to ensure that no app or service is left unturned in the drive to make sure that all digital data entry points are compliant. But perhaps just as importantly, it's crucial that they consider the user experience at every stage. By doing so, they can not only build and maintain services that meet the requirements of GDPR, but also ones that will make citizens feel more engaged and protected.

Preparing to reap the benefits

A number of forward looking councils are already well under way with their preparations for GDPR. They are doing so by looking positively at the benefits it will bring.

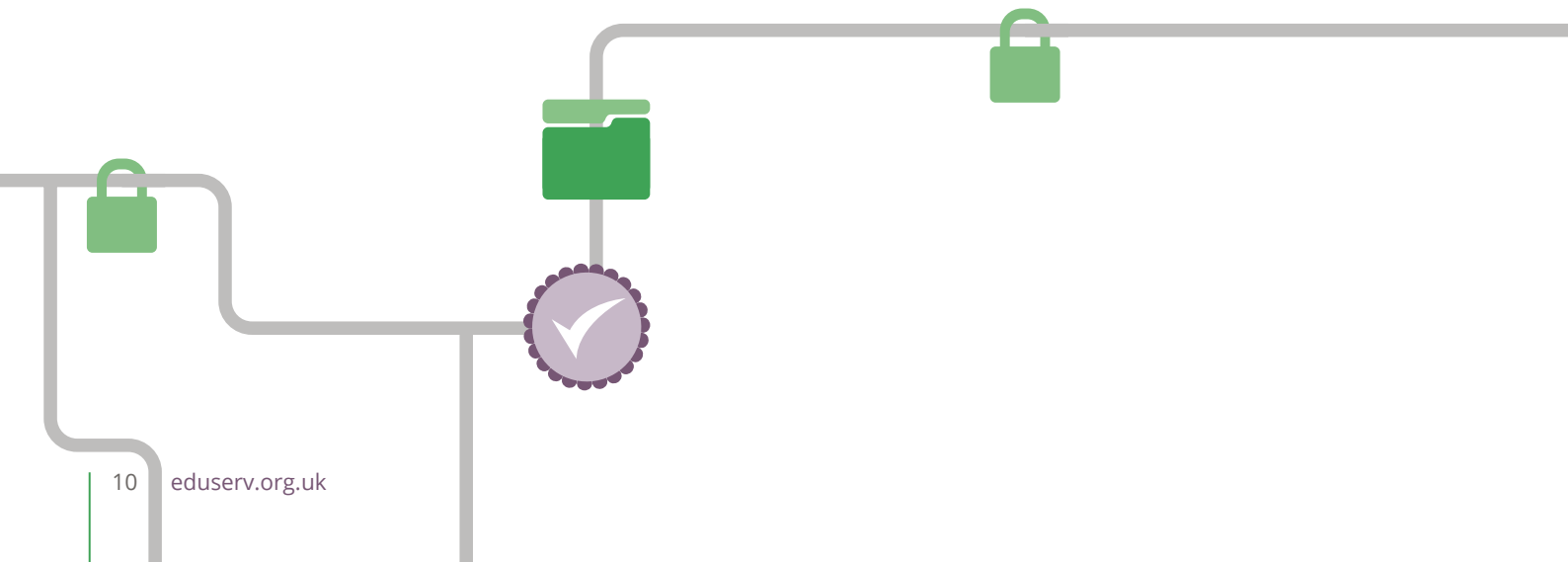
Rob Miller, CIO for Hackney Council, for example, says he's "hoping to use GDPR as an opportunity to put good data quality and insight at the heart of driving service improvement, rather than simply seeing it as a compliance exercise."

This is a view echoed by Lynn Wyeth, who is Head of Information Governance & Risk at Leicester City Council and is also Chair of the Leicestershire and Rutland Strategic Information Management Group.

> We see a real opportunity to identify where personal data is held in service areas... This will enable us to make sure robust contract clauses are in place and look for any gaps where written information sharing agreements may not have been implemented.

"We see a real opportunity as part of the GDPR work to identify, through an up to date information audit, where personal data is held in service areas," said Wyeth. "We will get a full picture of what conditions are used for processing (especially identifying where it is purely consent-based), where personal data is being processed as part of contracts and where information sharing is taking place. This will enable us to make sure robust contract clauses are in place and look for any gaps where written information sharing agreements may not have been implemented. Other benefits could include a refresh of retention and deletion schedules and some housekeeping undertaken to ensure that data are not being kept longer than necessary."

To make this happen the Leicestershire and Rutland Strategic Information Management Group has established a GDPR Task and Finish Group that has several work streams. This ensures that the GDPR preparation work is fairly spread out throughout all members in the county, so no one need 'reinvent the wheel' individually. It is hoped that this collaborative approach will also ensure consistency across the partner organisations within the Group when it comes implementation in May 2018.



Conclusion

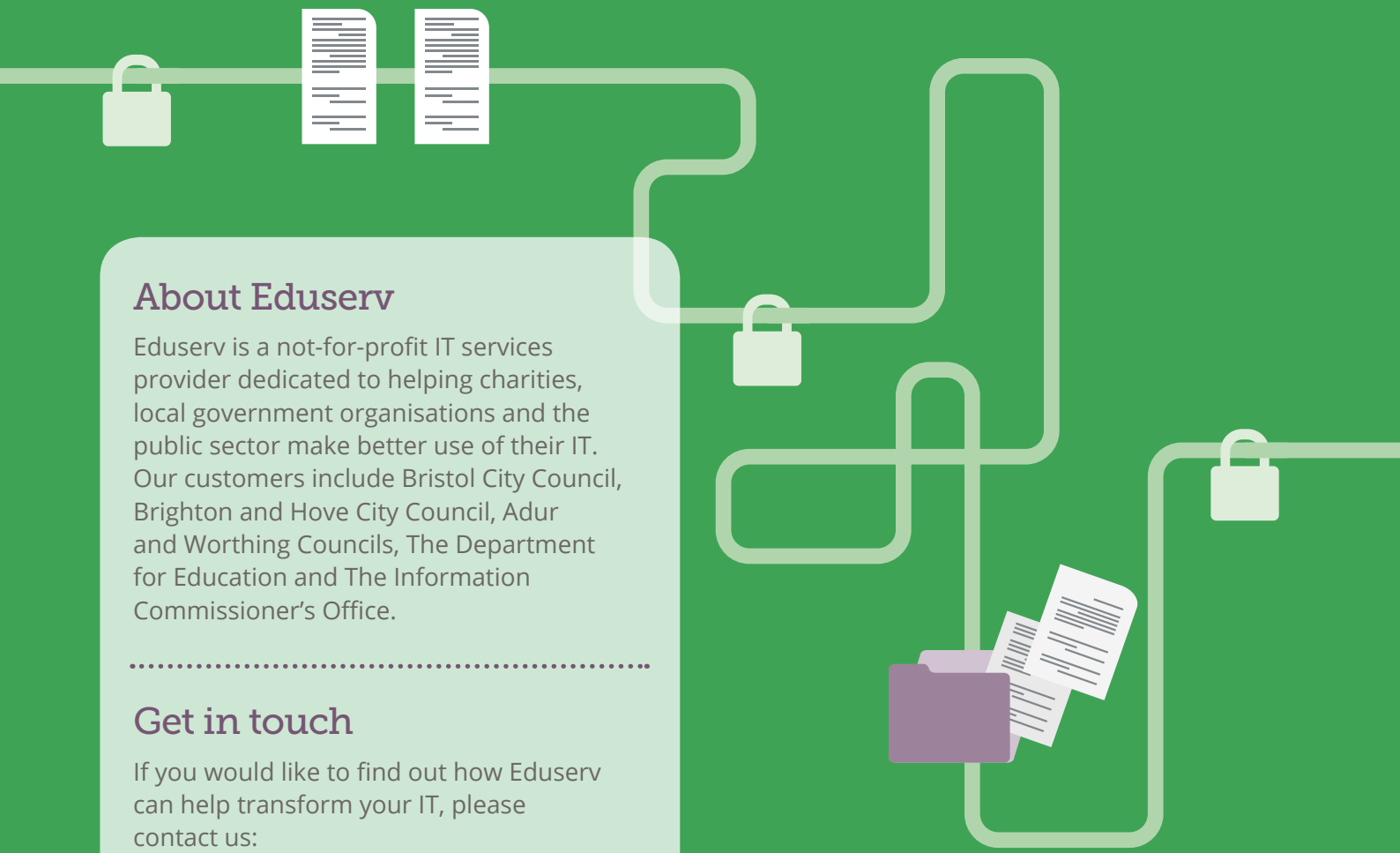
John Simcock, Head of Business Development for Eduserv

Currently, when you speak with CIOs you may find that compliance with GDPR is not always high on their priority list. Often, they are focused on transforming operations to deal with increasing demand for public services that need to be more despite shrinking budgets.

In some ways this is understandable. It's also a mistake, and it's because many commentators hace so far been guilty of talking about GDPR only in a negative way. GDPR is being seen as burden that has to be dealt with under sufferance, and only because you might get a larger fine if you don't comply.

This isn't the right way to look at things. GDPR needs to be far higher on council leadership agendas simply because it is the right and proper thing to do. As we've seen in this report, it could even make organisations more efficient and inspire trust in more efficient digital public services that could the key to future success.

I firmly believe councils need to see GDPR as an opportunity and grasp it as such. GDPR will ultimately make all much more effective in the way they manage, process and protect personal data. It could also help them use data more usefully for their own ends. In fact, I would go as far as saying that If organisations say they are intent on 'transforming' for a digital data-driven age, then GDPR can and should be a cornerstone of that effort.



About Eduserv

Eduserv is a not-for-profit IT services provider dedicated to helping charities, local government organisations and the public sector make better use of their IT. Our customers include Bristol City Council, Brighton and Hove City Council, Adur and Worthing Councils, The Department for Education and The Information Commissioner's Office.

Get in touch

If you would like to find out how Eduserv can help transform your IT, please contact us:

Tel: 0844 5000 115

Email: sales@eduserv.org.uk

eduserv

IT for public good

eduserv.org.uk

WEB-184.0