VERITAS

Turning GDPR from a Data Headache into an Information Opportunity

– Guidance for Local Authorities –

Prepared for Veritas by Jos Creese – CCL

CCL
Creating digital impact

CONTENTS:

Introduction

The EU General Data Protection Regulation (GDPR) comes into effect in 2018. It introduces a new set of requirements for all organisations who manage and hold personal data about EU citizens.

2018 is just a year away, and many organisations will need that time to prepare for the changes. It would be a mistake to think that GDPR won't apply because of Brexit. Not only will the UK still be part of the EU when GDPR comes into force, but it's now clear that the UK will choose to adopt GDPR in some form post-Brexit and it will certainly apply to local government as much as to business.

To view GDPR as just another administrative burden on business and government from the EU would be a missed opportunity. With the increasingly critical nature of information governance to protect reputation, privacy, and data assets, let alone to exploit the power of data to deliver better services, GDPR should be welcomed by organisations, if it is handled correctly.

Organisations that see GDPR as little more than a cost, are likely to waste time and effort 'ticking boxes' to appease auditors, and will potentially miss the opportunity to create new business value through improved information management.

Anecdotal evidence suggests that many councils are unclear what GDPR means for them, or how to prepare, or are simply avoiding acting in the expectation that GDPR simply won't apply to them. This report focusses on helping local councils to prepare for GDPR, providing a framework for suggested actions.

What is GDPR?

The General Data Protection Regulation (GDPR) seeks to harmonise data protection law across the EU. Currently, each country has its own rules and regulations - some more advanced and mature than others. It applies to any organisation in the world holding data about EU citizens – not just organisations in EU countries.

The UK Data Protection Act (DPA 1998) has been a leading example on data protection in Europe, but GDPR, which comes into force in May 2018, goes further than the current DPA, enhancing citizens' rights in knowing what data is held about them, and to have that data deleted (the 'right to be forgotten'). It brings in greater transparency, accountability and governance requirements, such as introducing a new obligation to notify data breaches (within 72 hours).

The data protection measures that the UK Information Commissioner's Office (ICO) has championed, such as privacy impact assessments (PIAs) and ‘privacy by design’, will become legal requirements under the GDPR for all organisations in certain circumstances.

The DPA is now nearly 20 years’ old, and has naturally begun to show its age. The GDPR brings the DPA up to date with more recent technology changes. For example, for the first time, specific categories of personal data are defined as in scope: an IP address can fall within the definition of what is personal data, as can genetic and biometric information.

The GDPR, like the DPA, applies to structured sets of manual records which contain personal data, where information about individuals can be identified by specific criteria. But it also outlines specific requirements regarding data collection that were not in the DPA – for example, that personal data must be given freely, not as a condition of receiving services, and that consent to collect, store and use data must be explicit, not implied.

Whilst the DPA allows citizens to make ‘subject access requests’ to see what data is held about them, for a fee, the GDPR goes further in making this more explicit, with a requirement to be able to have data extracted and sent in electronic format to the data subject, free of charge. So, we should all, in theory, be more in control of our data under GDPR, such as deciding if we want our data to be shared between service providers.

This is particularly important given growing public concerns about the connections made between apparently anonymised personal data and pseudonymised personal data, whether in areas such as retail or health services.

We all benefit from data being linked that allow public services to be better joined around our specific needs. As consumers, we are often prepared to give our private data, in order to receive more personalised services that reflect our preferences. However, these data linkages which combine sets of private data, can result in privacy risks. GDPR introduces more specific controls, definitions and checks to help avoid this digital opportunity leading to our personal data being exploited against our wishes.

The real challenge for organisations lies in being able to show that they have the systems, controls and the records in place, to comply, not just to be fortunate enough to avoid a data breach ‘by hook or by crook’. The new ‘accountability principle’ in GDPR requires organisations to prove their compliance, for example, by undertaking staff training, audits, maintaining documentation on processing activities, and having appropriate and auditable information governance policies and processes in place.

Failure to comply may be proven only if there is a serious data breach – but with the potential of fines being levied, let alone the impact on reputation, ignoring GDPR would be a risky option for councils.

Will Brexit exempt the UK?

Some councils are not yet convinced GDPR will apply – after all, it's an EU regulation and the UK is leaving the EU. We already have the DPA – what more is needed? However, in January 2017 the ICO confirmed that GDPR will apply (see their website):

> ***"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. The ICO is committed to assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond. We acknowledge that there may still be questions about how the GDPR would apply in the UK on leaving the EU, but this should not distract from the important task of compliance with the GDPR."***
>
> ***WWW.ICO.Org.UK, Jan 2017***

The Prime Minister, Teresa May has said that she is putting before Parliament the Great Repeal Bill. This, when passed into law, will both repeal the European Communities Act (which would mean that EU law no longer had direct application in the UK), and implement the very same body of law into English law. Although it is possible that amendments could be made to existing EU laws, such as the GDPR at the same time, the likelihood is that wholesale amendments will not be made until some time later, when the Brexit 'dust' has settled. So, the undiluted provisions of the GDPR are likely to remain applicable to councils (and all other UK organisations) post-Brexit.

In any event, councils already hold an increasingly complex array of inter-linked data that requires care in dealing with personal data:

- Sharing services and functions, or processing data on behalf of one another
- Connecting datasets together for new insight across a range of public services, for policy planning and better service delivery
- Using data and information to target services, goods and early intervention, for reasons of improved efficiency, revenue collection or as new commercial opportunities emerge.

For all these reasons, it would be unwise for councils to ignore GDPR. It is better to understand its impact and plan for changes in internal information governance now, rather than to risk playing 'catch up' later.

Isn't it just good practice?

To do business with the EU in the most efficient manner, the UK will need the EU Commission to make a finding that the UK's law on data protection is adequate: this means that the protection offered is in line with the GDPR.

The GDPR is designed for the digital world, where personal data is increasingly held electronically, with potentially significant new marketing and public service improvement opportunities. Councils are moving ahead quickly in adopting digital methods of working, with growing numbers of systems designed for automated self-service and making logical connections across related services for their citizens.

For this to be successful, the public must trust how councils use and hold that data – that it is secure and used responsibly. Without that trust, citizens are much less likely to agree to share their personal data or to choose to transact electronically. This would be disastrous for councils now relying on digital delivery to help meet growing demands for services whilst at the same time finding unprecedented efficiencies because of cuts.

Take for example, the health service and council plans to digitise care records. If we don't believe those systems are secure, that our data is kept up to date, shared appropriately and safely, and that we can find out who holds what data about us, then the plans to digitise health services just won't work. The well-intentioned but poorly executed Care.Data programme is a good example of a failure of trust from citizens and practitioners alike.

With the growing importance of using personal data, and the risks associated with it, the ICO is working ever more closely with regulators in other countries - to protect UK citizens and our economic interests. The UK digital economy will depend on it, and so will the security of UK digital citizens increasingly at risk from international fraud and cybercrime.

In November 2016 Computing magazine investigated the priorities for business leaders regarding data security. For large organisations with more than 500 staff, GDPR was top of the list. For smaller organisations, disaster recovery and user awareness of security were higher concerns. That pattern is likely to be the same for local government.

Larger councils, such as county councils and unitary councils, may find GDPR particularly challenging, because citizen data will be spread over many systems and departments, and although current law would require them to find this data, the increased fines in GDPRand more stringent requirements increase this risk.

But proliferation of digital records held across multiple systems, located in the cloud or on premise, is not unique to larger organisations. Identifying, extracting or erasing all data about someone on request is a complex task, and so for all organisations GDPR compliance requires rigour in information management practice.

Any council that suffers a serious data breach and cannot subsequently demonstrate that it had taken sufficient steps to avoid being found negligent, will be liable to significant fines. But the reputational damage is likely to be at least as serious.

The wide-ranging implications of GDPR regulations on processes, systems and IT support, means that it is a non-trivial challenge to comply for all but the smallest and simplest organisations (and even very small councils are complex by their nature). For example, lots of redundant data, or poor quality data, or simply not knowing where data is located, may mean personal data is held but not easily identifiable.

How to prepare for GDPR

There are some key areas for councils to consider in preparing for GDPR (and plenty of online guides to help with the detail):

1. Firstly, if you are processing data, then GDPR requires you to maintain records of all personally identifiable information and how you are using it. If you are a data controller (i.e. you specify how data is processed, say to a partner, supplier or outsourcer), then you must ensure every contract you have with a data processor complies with GDPR.
2. Secondly, you need to have clear responsibilities in place for data owners - responsibility for knowing where data is physically located, for maintaining quality and for its life-cycle management. All councils should have a senior information risk officer (SIRO), ensuring board level accountability and understanding of information risk. Responsibility should also extend to employees – everyone has a duty of care when it comes to information, and that should be clear in HR policies as well as in training plans.
3. Thirdly, councils should review and update their information management policies and practices. This includes specific aspects, such as breach notification processes, as well as general good practice – such as data handling and sharing, security and privacy controls, use of open data, maintaining data quality, common formats for data types, 'capture once, use many times', and so forth. A simple set of information management principles covering these areas, agreed with the board or council management team, and administered across the council, (which indeed should already be a feature of any council's compliance regime) can reduce costs and risks of GDPR compliance.
4. Lastly, good information management tools are needed to avoid unnecessary manual overheads – reporting and tracking, securing transmission and data sharing tools. This includes interrogation and reporting tools, open APIs, access and security methods across the whole council. This will also allow services such as cloud to be used where appropriate with confidence that data controls are not being broken. Some of these will lie within the IT department for managing data and systems architectures effectively. But there are also tools needed by business professionals in departments, and for specialists such as the legal services teams.

This approach will not only will help with GDPR compliance, but also ensure good information management practice in any organisation. It reduces business risk, whilst also increasing employee productivity and efficiency by giving information access securely, to those who need it, when and where they need it. That, in turn, improves decision making, customer service and business agility.

The challenge then for those officers in councils tasked with information and GDPR compliance, (and you should have a Data Protection Officer) is to persuade the executive board and councillors of the priority to justify the necessary resources and commitment in order to fulfil the responsibility. That means selling the value of information management and GDPR compliance as a business benefit, not as an unavoidable regulatory and statutory compliance issue, with the threat of potential fines.

Who's responsible?

Many councils are not clear about who is responsible for information. The CIO, IT, Legal Services, SIRO, system owners, specific departmental directors and Data Protection Officers, amongst others, all have a role. In some councils, there is also a Privacy Officer, or internal auditor given specific responsibility for advising on information compliance.

Councils with social services departments and health organisations will also have appointed a 'Caldicott Guardian', a senior person responsible for protecting the confidentiality of information relating to patient and social care service users, including enabling appropriate information sharing.

In the private sector, there is a growing trend to appoint a Chief Data Officer at board level to oversee the function, but this is still uncommon in local government.

Under GDPR, all public authorities and larger processing bodies must appoint a Data Protection Officer (DPO). Such an appointment can be shared, where, for example, local public services are already in shared service arrangements. The DPO role is to oversee GDPR compliance and to act as a contact point for employees and customers. The DPO is expected to report to a board level individual, yet operate with a degree of independence and autonomy. As such, the role is broader than the DPO function that already exists in councils today.

In some councils, the role is given to the CIO (after all, that means "Chief *Information* Officer"), Head of IT or Chief Digital Officer. In whatever way that a council approaches this, two requirements are key:

- Someone at board level responsible for information - as a risk and an asset, setting policy, practice and good data/information use and awareness.

- Someone in IT responsible for ensuring systems, technologies, data handling tools and security practices comply with agreed information policies.

These should not be the same person.

Other areas also have an interest and responsibilities - Marketing, HR, Finance, CEO, Legal. All these professional areas need to be aware and actively working together to ensure compliance. Setting a single budget for securing GDPR compliance is a good place to start to ensure this integration and collaboration occurs without blurring responsibilities.

What should CIOs do?

Councils CIOs are heavily engaged at present in transformation programmes, modernising their IT estates and cutting costs in IT and across the business.

But it would be a mistake for a council CIO to downgrade the priority of GDPR in the face of this barrage of work, given the growing importance for councils of good information governance, protection of data and the need to ensure privacy for all personal data.

There are some basic things CIOs can do specifically, to help the council to get ready:

- Know where systems data resides: ensure systems owners are aware of data assets, provide tools to assist with master data management (MDM) and data cleansing, to improve data quality, data protection and know where it is being stored, how it is being used and for how long it needs to be kept.
- Ensure policies exist and can be enacted in practice, for data retention and deletion. Storing everything for ever may be affordable, but is already illegal in relation to personal data, and represents a growing liability. IT needs to provide the tools for information risk management, even if IT is not directly responsible for the risk itself.
- Help the executive board and non-IT leaders to understand how to manage information risk - quantification, monitoring and mitigation. Having a coherent information architecture, agreed processes for data handling and a set of information management principles can reduce risk.
- Support data mapping activities - not just being able to pinpoint where data resides, but for example data in transit, data linkages across applications, and data flows which involve data sharing.

HR policies should ensure that employee responsibility regarding data use and handling is clear and taken seriously - and sanctions exist for poor habits. HR can also assist by providing training and mentoring support. IT can help HR colleagues in councils to prepare for GDPR.

Unless there has already been a serious data breach or ‘near miss’, then simply asking the council for new money to comply with a new GDPR EU Regulation is perhaps not the best approach. The reaction is likely to be "*what is the minimum we need to do to be seen to be compliant?*". It might be tempting to adjust policies but not to also change working practices.

The potential GDPR fines are set at a level designed to ensure that organisations do not simply weigh up the costs of compliance against the amount of the fine. Yet the threat of fines may not be enough to make some boards invest to ensure compliance, including buying in outside help and updating or replacing systems where this is required.

Therefore, to maximise the chances of success in securing corporate support, it is important to turn this into an opportunity to promote the benefits of strong and effective information governance, which delivers GDPR compliance as a bonus.

After all, good information management practices are often patchy in councils, focussing on areas such as Caldicott Guardian and individual departmental systems or known risks, rather than a holistic approach to all data and information, paper and electronic, in every area and system, held internally or externally.

Building a business case

Despite the potential to increase information value and to reduce unnecessary data management risks and overheads, there is still a cost to GDPR compliance. For councils already facing enormous cuts and a need to reduce or to remove overheads, making the case for a programme to secure GDPR compliance is not easy.

A council business case for investing for GDPR readiness should therefore fall into three parts:

- **Building on ‘Business as usual’** .. the existing good information and data management practices (hopefully already in place) and getting better value from existing information assets and projects – managing risks and opportunities and being more streamlined and consistent in how we do it. In other words, doing a bit more of what we do already to align with GDPR and address obvious short-comings.
- **Building Awareness across the council** .. defining how GDPR can help to meet citizen expectations regarding their data, where the risks lie and how to manage them better, as well as the penalties and downstream costs of a failure to comply. This awareness will help to understand why GDPR matters, balancing the benefits against the risk of non-compliance and a potential for fines.
- **Undertaking a gap analysis** .. establishing where the main weaknesses lie in current policy and practice and how these can be addressed – prioritising the aspects which have the greatest risk, benefit or urgency. This should connect the first two items

(where we are today and what GDPR means for us), so that the board can understand GDPR in the context of business ambitions.

In other words:

> ***Investing appropriately in improved information governance will pay off by being able to deliver better services, more efficiently and flexibly. It will also avoid the risks, reputational damage and potential fines from not complying with GDPR.***

Taking action

All organisations vary and therefore need their own individual plans to meet the requirements of GDPR in time for its adoption in 2018. But here is a suggested checklist of some of the main things to assist in that planning, covering policy, practice, governance and technology actions. It is provided, to assist DPOs (or whoever is leading on GDPR compliance) to build their own coherent plan of action:

	Actions Suggested:	✓
Policy	• Undertake a review of existing corporate policies which are affected by GDPR (IT, HR, procurement, privacy notices, audit, specialist areas such as social care). Make any necessary changes in time for GDPR implementation.	
	• Review policies regarding data: collection, retention, handling and sharing to ensure that these are tested for GDPR compliance, especially concerning the rights of data subjects, such as explicit and informed consent.	
	• Check the adequacy of existing policies for data subject consent, e.g. being informed, ambiguous and freely given, and this applies to children's data (which implies specific action regarding parents and guardians).	
	• Ensure that policies and procedures are in place and tested regarding how to manage data breaches.	

	• Consider adopting ICO recommended good practice of ‘privacy by design’ approach and carry out Privacy Impact Assessment as part of this – see the ICO website for more details.	
	• Ensure clear definitions exist of ‘sensitive and personal data’ consistent with GDPR definitions for relevant data sets.	
Practice	• Undertake checks on suppliers if they are processing data on behalf of the council, such as cloud providers and outsourcers, to confirm they are complying with GDPR.	
	• Test all internal procedures to deal with subject access requests (the right to know what data is held, consent, and deletion).	
	• Ensure a tested ‘consent to collect, use and to share’ process is in place and auditable.	
	• Ensure that all the organisation is aware of information governance responsibilities regarding personal data and GDPR impact.	
	• Put in place a compliance project with a named project manager and necessary funding to deliver in time for May 2018.	
	• Undertake an audit of legacy data – where it resides, where consent has been given (or not), and actions to deal with any shortcomings in relation to GDPR compliance.	
	• Document what personal data is held in all departmental areas and systems, where it came from, and how it is used/shared.	
	• Ensure that you know the legal basis for which personal data is held, and that this is documented.	
	• Put in place procedures for managing data quality, such as correcting data errors. Consider using ‘Master Data Management’ (MDM) methods. This should include working with other organisations with whom data is shared to ensure data quality management practices.	
	• Undertake and document specific tests to check procedures deliver on policy commitments, such as ensuring that data subject access requests can be dealt with within the 72 hours’ time limit.	
Governance	• Ensure all information governance roles and reporting structures are in place, where required, to deliver GDPR compliance. This should include a designated Data Protection Officer (DPO) and clarity of roles within IT, areas such as social care and functions with responsibility for personal data.	
	• Ensure that someone at board level is responsible overall for information governance and GDPR compliance and a DPO has specific responsibility for GDPR and ICO interface (including the GDPR compliance programme).	
	• Determine the reporting lines for dealing with breaches, the review of the evidence of audit trials and routine tests of compliance with policy.	
	• Ensure that senior professionals across the council are aware of GDPR legal implications and that the council’s risk register is adjusted accordingly.	

Technology	• Ensure system tools are in place to identify, extract, delete and report on personal data, as required (to meet access requests, to correct data errors, to erase data etc).	
	• Ensure IT management practices and support underpin good security and information protection – network and systems access, accreditation, system patching, upgrades and system selection, ID management, change control, penetration testing, audit, intrusion detection, reporting and incident management.	
	• Review all IT contracts and the obligations on suppliers to ensure appropriate GDPR compliance, with appropriate actions to deal with any legacy issues in existing contracts.	
	• Ensure that systems procurement and specifications allow for the necessary identification and management of personal data to meet GDPR obligations.	
	• Adopt common data formats across all systems and information to make individual personal data identifiable across system areas and business functions.	
	• Consider developing online systems that allow people to search for their own data through self-service online, and put in place intuitive and easy to use subject access request forms.	

Conclusions

Councils have already faced much change over the last decade. Budget cuts have forced some services to be stopped entirely and others have been redesigned and streamlined. This has included moving to digital operating models, creating new public/private partnerships and adopting shared services.

Although the focus has been mostly on process simplification and automation, information management is now an essential part of achieving wider efficiency, service improvement and improved risk management.

Good information management practice helps to ensure that council staff have the data and tools they need to be more productive and effective in their jobs. It also improves democratic accountability and transparency, as well as giving citizens easier access to joined-up digital services which they can use with confidence, security and privacy.

Information disciplines are also now essential for the adoption of new technologies and digital methods – such as cloud, social media, apps, channel shift and more; indeed, it is mostly the fear over data access, control, security, location and management that explains low cloud adoption by councils.

Poor information practice also carries a variety of risks for all organisations, from data misuse, reputational damage, or risks to vulnerable people using services. Addressing the challenge of GDPR should be a way of sharpening information practices in councils, making it a ‘business opportunity’, rather than just another government regulatory overhead.

Indeed, in the future it is quite likely that some form of kite-marked data management competency will be a requirement of public services holding and using identifiable citizen data – this could be GDPR compliance or ISO information management accreditation.

Finally, councils should assume that GDPR will apply to them – Brexit is not a 'get out of jail' card, the ICO says GDPR will apply, and councils are unlikely to be exempt in any case. Therefore, preparation needs to start now, with a clear case made for GDPR to improve information governance as a business need, not just to secure compliance to avoid the risk of a fine.

About the author

Jos has worked for county, district and unitary councils as well as central government. For over a decade until 2015 he was CIO and CDO for Hampshire County Council. He is a past president of Socitm and the immediate past President of BCS (2015), the Chartered Institute for IT.

Jos worked on national government digital programmes and has led large-scale mergers, international IT programmes and the start-up and subsequent sale of a tech business. His work has included developing technology, information and digital strategies across the public sector, especially to support transformation and shared Services underpinned by commercial models.

In 2010 he was listed as the 'most influential and innovative CIO' in the UK in the 'Silicon 50' CIO survey and included in the 'Top 100 CIO' list since its inception until becoming a consultant.

Having held various CIO and non-executive director positions, Jos is now an independent consultant, providing expert advice to public and private sectors on digital and IT strategy – helping the public and the private sectors to work better together.

This includes helping local public service to sharpen their commercial and business practice, and helping the private sector to understand what is needed in a fast-changing public sector.

Twitter: @JosCreese
LinkedIn: http://uk.linkedin.com/in/joscreese

CCL
Creating digital impact

About Veritas

The exponential growth of data and the resources needed to manage it is one of the most pressing issues facing business today. And it's not just the amount of data. It's where it lives and how it travels between private clouds, public clouds and back to on premises. In these increasingly complex IT environments, it's important to focus on what's constant: the data.

Every one of our information management solutions – from business continuity to back up and recovery to software defined storage and information governance – is designed around the principle that information is more important than infrastructure. Veritas has the privilege to help the world's organizations - including 86% of the global Fortune 500 - collect, protect, analyze and optimize their data, even in the most demanding environments.

www.veritas.com