Records Management Perspectives: Leaving the digital Stone Age behind

How to prepare for the EU General Data Protection Regulation

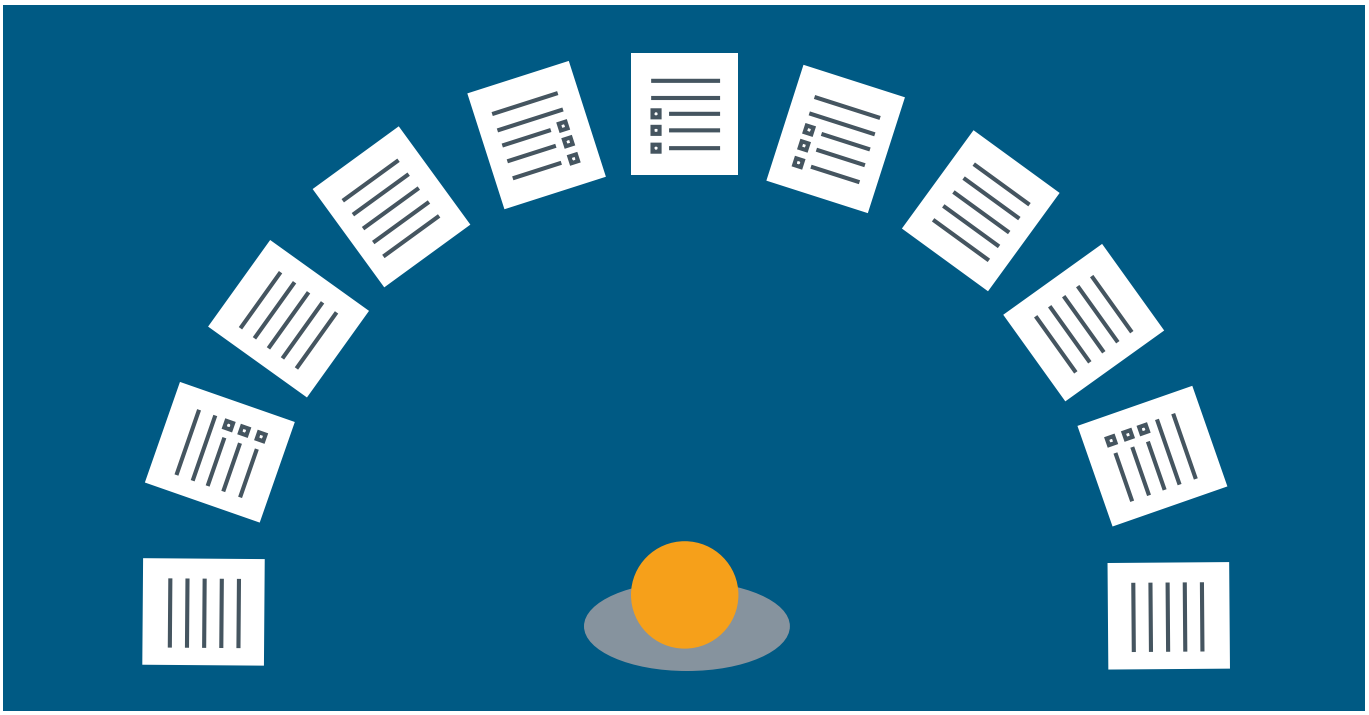
By John Culkin
Director of Information Management

The power of memory

www.crownrms.com

CROWN RECORDS MANAGEMENT

A NEW ERA FOR DATA



A challenge for all businesses that collect or use data

It's no wonder that data legislation from nearly 20 years ago is out of touch with the realities and demands of modern life, both from a consumer and business perspective. Technological developments are responsible for the generation of vast amounts of data, bringing with it questions around privacy and data protection - fuelling the argument that it's time to leave the digital Stone Age behind.

"The message the European Parliament is sending is unequivocal: this reform is a necessity, and now it is irreversible."

The words of European Commission Vice President Viviane Reding, following a decisive vote in favour of a new EU Data Protection Regulation, are unequivocal. Yet businesses across the UK appear to be in denial as they await the adoption of changes that will have huge implications across every sector.

The new regulations still have to be ratified by the Council of Ministers and could be altered or diluted in the coming months. The message coming from Europe is they will be approved in one form or another during the course of 2015 and in place by 2017 - bringing today's data protection rules from a digital Stone Age towards a modern era.

One trillion Euros

The desire for new laws is driven by a recent explosion in data. Prompting predictions that personal data of European citizens could be worth **ONE TRILLION EUROS** a year by 2020. There are also growing fears that individuals are losing control over personal data - becoming a commodity in its own right.

The legislation replacing the current Data Protection Act in the UK, which has been in place since 1998 – aims **to provide a Europe-wide regulation for data controllers and processors.** It will provide a one-stop shop to deal with a single **Data Protection Authority** in each country and new **European Data Seals** – a kind of 'kite mark' to show a company's processes are in order, helping to aid compliancy.

It will also provide citizens with a **'right to be forgotten'** if they want old or inaccurate data deleted. A right to know what information is stored about them and whether it is correct - as well as a right for transparency in the way data is collected.

So the big question for every CIO, IT Manager, Office Manager and every CEO across all sectors is: **are you ready to leave the digital Stone Age behind?**

Whether we are talking about the financial services, healthcare, legal, manufacturing or public sectors, this legislation is coming. Having major implications not only for the way data is handled, processed and stored but also how to deal with requests from individual citizens to search, delete or forward data – not to mention operational budgets.

Hard-copy data not exempt

It is worth noting that the regulations not only apply to digital data; they also apply to physically-stored data - if it forms part of a relevant 'file system' which may be far more difficult to search or locate.

The bottom line is these issues need to be taken into consideration. In fact, the sooner the better if businesses don't want to be caught out when new regulations are finally adopted. **Playing the waiting game could be a risky option.**

Key proposals:

- The setting up of a single Data Protection Authority (DPA) for each country and a European Data Protection Board to co-ordinate DPAs.
- Fines of up to 5 per cent of global turnover for companies that intentionally or negligently breach regulations.
- Explicit consent to be sought from individuals before data can be collected. Consent for children under 13 must be provided by a parent or guardian. Data subjects to have the right to withdraw consent at any time.
- Controllers must provide the data subject with the purposes of collecting their data, the period for which it will be stored and advice on their rights for information to be deleted. They should also be told who will receive the data and whether the controller intends to transfer it to a third party.
- Data subjects to have the right for inaccurate information to be corrected.
- The 'right to be forgotten' to be granted, allowing data subjects the right to ask for old data to be deleted, and a 'right to data portability', so individuals can request their information in a useable format.
- A requirement for 'privacy by design' in the way data processing systems are operated.
- A requirement for data breaches to be reported to the supervisory authority within 24 hours and to data subjects without delay. Processors should inform controllers immediately.
- All companies with more than 250 employees, and those whose core activity requires systematic monitoring of data subjects, will need to appoint a Data Protection Officer.
- Data protection certification and data protection seals to be introduced to aid compliance.

ON MY WAY, READY OR NOT

Data reform will touch every sector

It doesn't take Sherlock Holmes to answer the question "is British business ready for EU Data Protection Regulation?" Anecdotal evidence alone suggests IT departments and CIOs across the country have been taking a 'wait and see' approach, while others have simply ignored it altogether. This short-sighted policy is a worrying trend, not least because if companies fail to implement a robust data policy in time it could lead to huge fines.

Even sectors with a keen eye on the political agenda seem to have been wary of implementing recommendations early and have instead lobbied for changes. The NHS European Office and Royal College of Physicians issued a joint statement fearing the Regulation's requirement for 'explicit consent' could affect the sharing of patient data and damage scientific health research.

A wake up call for businesses

It's worrying to see how little is known about the new regulations ahead. The changes will affect every organisation and the duty to comply falls to everyone – this is not just an IT issue. Companies need to 'wake up' and start taking action to avoid any nasty impact on their business and to avoid breaches in the future.

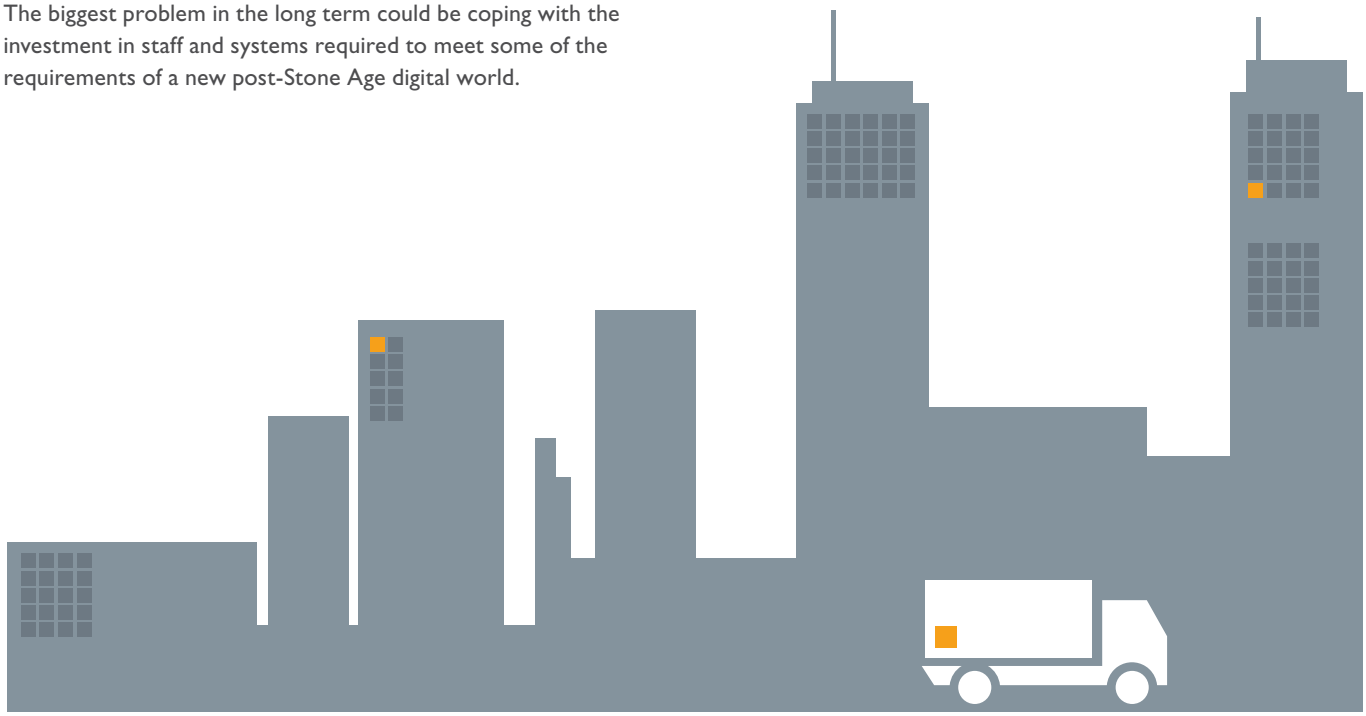
It isn't all negative, of course. The regulation will provide organisations with a chance to improve efficiency through better, cleaner data – while users will have more control over information stored about them.

The biggest problem in the long term could be coping with the investment in staff and systems required to meet some of the requirements of a new post-Stone Age digital world.

The stats: British IT decision makers in the dark over EU data regulation*

- 50 per cent of British IT decision makers are completely unaware of the forthcoming legislation
- Only 10 per cent said they fully understood what steps needed to be taken to be compliant
- 85 per cent of UK respondents believe their organisation faces 'significant challenges' to comply
- Almost a quarter of UK respondents were unaware of proposed fines for failing to comply

** Source: Trend Micro survey of 850 senior IT decision makers across Europe, April 2014.*



Rights are changing

Articles 14-17 of the EU's Data Protection Regulation (there are 88 articles in all) deal with the rights of individual citizens, including the famous 'right to be forgotten'.

These provide a right of access to information, a right for inaccurate information to be corrected and rights for certain information to be 'forgotten' or deleted. Add in a right for individuals to withdraw consent for information to be stored at any stage, and it is clear companies across all sectors face a potential headache in dealing with the sheer volume of requests that could come their way.

You only have to look at how the Freedom of Information Act has impacted on many organisations, especially the public sector, to realise what is in store. While an FOI request often incurs a nominal charge, it is currently unclear whether similar charges will be permissible, especially for commercial organisations.

With individuals given a right to ask to be presented with their data in a useable format, this has further financial implications - underlining the need for businesses to take greater interest in the legislation.

Outside of the EU – but still in the net

A controversial aspect of the EU Data Protection Regulation is that it attempts to control European citizens' data held outside the EU as well as inside it; requiring any company that uses the data of Europeans to comply.

This could be relevant, for instance, to the monitoring of Europeans through cookies by companies outside the territory carrying out marketing activities.

A major change in emphasis means that not only the data controller could face sanctions but the processor too. Whereas now a data processor can assume the controller bears the responsibility of paying fines, this may no longer be the case.

Reading your rights – key clauses and what they mean

Article 14
Information to the data subject
When collecting data, controllers must provide the data subject with the following:

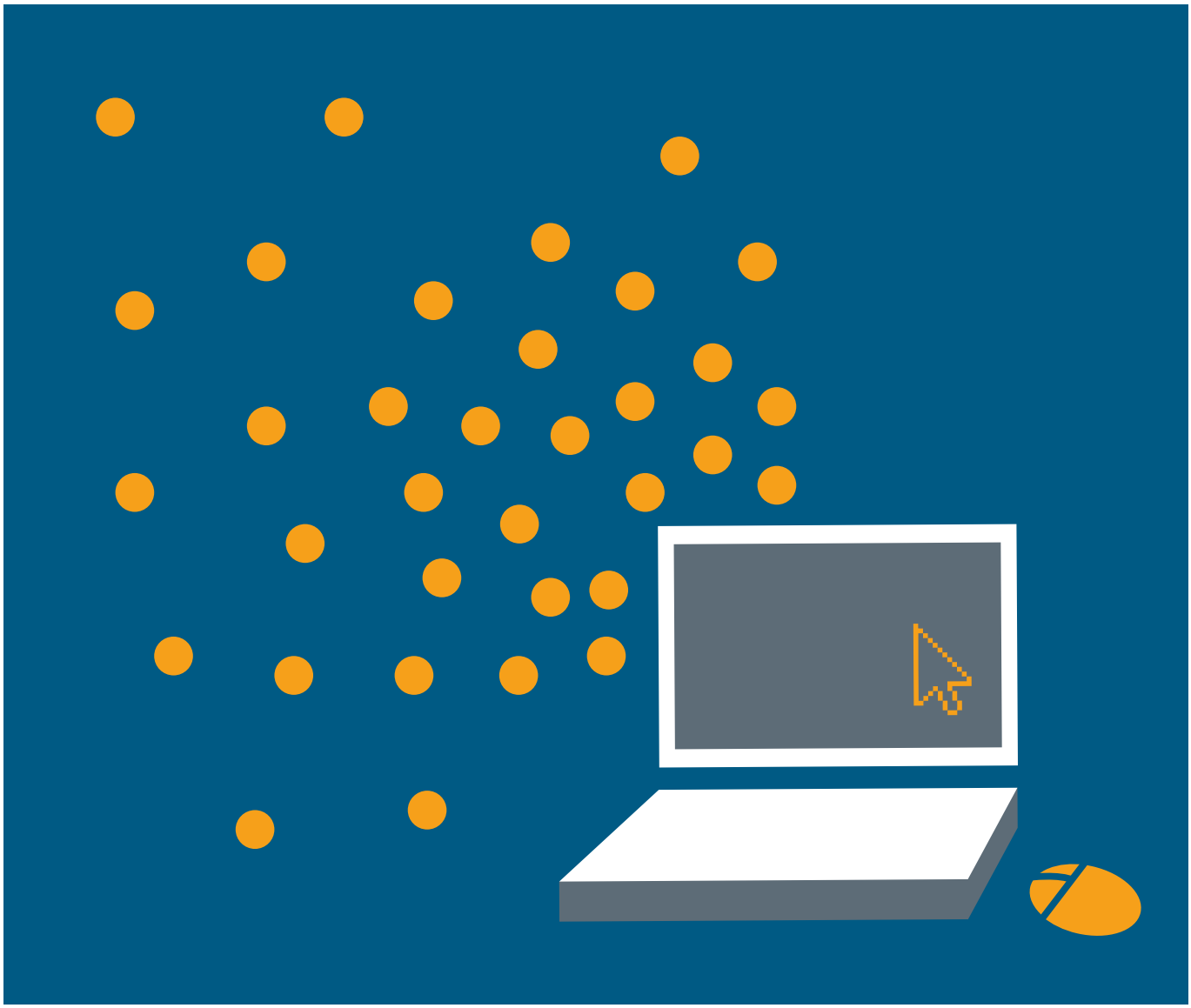
- identity and contact details of the controller or representative
- purposes of collecting the data
- the period for which it will be stored
- advice on their right for information to be deleted
- details on their right to complain
- who will receive the data and whether the controller intends to transfer it to a third party.

Article 15
Right of access for the data subject
The data subject has the right to obtain - at any time - details of information being processed about them.

Article 16
Right to rectification
Data subjects have the right for inaccurate information to be corrected.

Article 17
Right to be forgotten and to erasure
The right to ask for data to be deleted is to be introduced, especially information collected when data subjects were still a child. Controllers must take 'all reasonable steps' to remove it. Controllers will also be responsible for third parties authorised to use the data.

SIX STEPS TO A NEW DATA WORLD



Grasp the opportunity ahead of time

For all the scare stories about data regulation reform, including the procedural challenges and financial impact it will inevitably bring, this is not a time to panic. Instead it should be seen by companies and their CIOs as an opportunity to once and for all take charge of the physical and digital data in their organisation, and make it work as a business asset.

Even if the proposal passes into law in December 2014, which is at the earliest possible opportunity, the process of enactment could take up to a further two years - leaving a long window for preparation and no need for knee-jerk reactions.

Waiting until the last minute, however, is neither necessary nor advisable. The important point to consider is that although at this stage the finer details of new legislation are not yet clear, the direction of travel is not in doubt: Europe wants more rights for individuals - and citizens are increasingly demanding it.

With that in mind, there could be significant benefits for companies who get their house in order early and begin to offer customers what they want – a right to have some control over their data and a right to ask for it to be corrected or deleted. It would be foolish not to think early about how to comply with such demands in future.

Six steps to protecting your corporate memory

We recognise the value of data and protecting 'corporate memory'. Below are six key areas in which businesses can prepare for all eventualities in an ever-changing data environment by adopting basic principles of data collection, storage and destruction.

These are steps which will not only place companies and organisations in good stead when the new EU Data Protection Regulation finally becomes enshrined in law, but will also have a positive impact on operational health.

1. **Spring-clean your data: understand its value**
   Start with an audit to distinguish how much data currently stored actually needs to be kept. Is it 'records' or in fact junk or data noise? Destroying unnecessary information can help create a clearer picture for the future. For data that needs to be kept, make sure you know where it is stored, who uses it, how to access it and how to protect it. The key to good data practice is in understanding its value in the first place; so treat data like an asset. You wouldn't leave an asset in the street for other people to pick up - and it is no different in a digital environment.

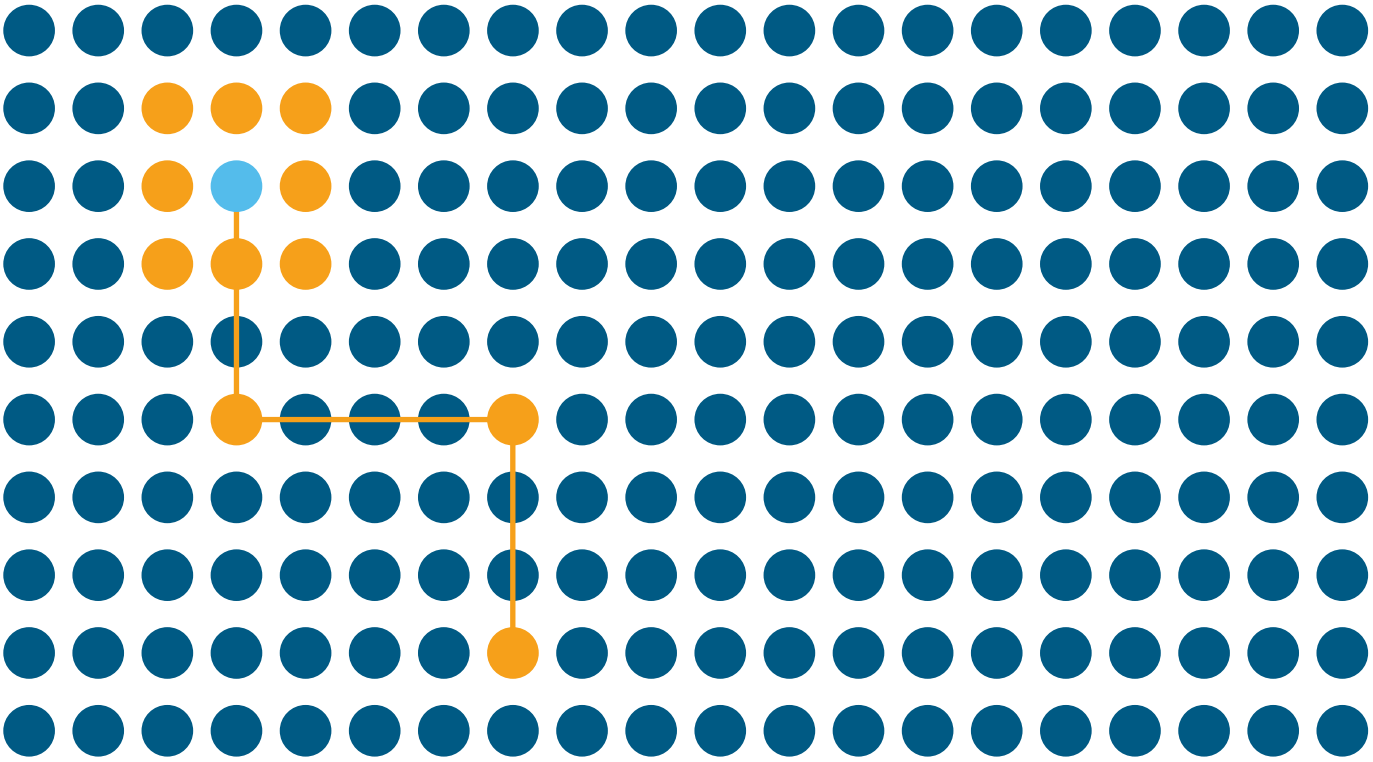
2. **Know who is responsible: assign ownership**
   With fines for non-compliance set at up to 5 per cent of global annual turnover it's vitally important that someone in the business takes ownership and responsibility for staying up to date with new regulations. Make it clear which role in your business has responsibility for each type of data - whether it is the IT Manager, CIO, Records Manager, Office Manager or an outsourced company.

3. **Develop processes now to deal with data breaches: be prepared**
   It will soon become compulsory for all companies in the EU to have a system in place for dealing with data breaches, including processes for notifying anyone affected by a breach. So why wait? Clear and well-practised procedures should be put in place now – not least to identify who is responsible for reporting.

4. **Create a guardian angel of all things data: seek advice from an expert**
   Under current plans any organisation with more than 250 staff will have to appoint a Data Protection Officer – but all companies should think about seeking expert advice at the very least. If you don't want to hire a dedicated angel, you can outsource to a trusted partner. Crown Records Management, for instance, offers an IM6 audit designed to assess the data management health of businesses and suggest improvements that can be made.

5. **Understand whose data it is: seek consent and open communication channels**
   In the future companies will require explicit consent from people to gather their personal data; so get those processes in place early. Any company storing personal data should consider what the legitimate grounds for its retention are, and how they will communicate this to customers as we move inevitably from implicit consent to explicit consent.

6. **Design in-privacy : change your culture**
   Start to create a company culture where privacy is considered in every process and at every level of the business. Designing in privacy and making staff aware of its importance - is the key to good data practice as data protection evolves.



The bottom line is the age of data is changing fast, for better or worse and whether we like it or not. So regardless of what ministers in Europe decide over the coming months - and however the final EU Data Protection Regulation takes shape - the digital Stone Age is on the way out.

For those who view it as an operational nightmare, the challenges are multiple. But for those who grasp the nettle and see it as an opportunity to truly value data as an information asset, the positives are equally clear. It could yet prove to be a brave new data world.