GDPR: New strategies for data protection
What you need to know and what you need to do next

By Chris Scott - Data Protection Officer, The Bunker

JUNE 2017
Contents

Chapter 1: What is the General Data Protection Regulation (GDPR) – a reminder

Chapter 2: The impact of GDPR on people, processes & technology

Chapter 3: Backup, recovery, accessibility & how to forget people

Chapter 4: Notification of breach

Chapter 5: How to get GDPR ready

Conclusion

About us
Chapter 1: What is GDPR – a reminder

In the 1990s, the web was a place of anonymity. “On the internet, nobody knows you’re a dog,” a famous New Yorker magazine cartoon joked in 1993.

But things have changed since then. Today, everyone knows you’re a dog. Businesses routinely gather, store and analyse online information about consumers, often without their knowledge. And there are growing concerns about the way that third-party profiling websites, as well as tools used by businesses to ‘mine’ opinions, views and sentiment about their brands online and on social media, are creating vast, and largely unregulated, stores of personal information.

Did you know?
There are apparently four web analytics companies tracking users as they visit pages on the NHS Choices website.

Now, the European Commission (EC) is getting ready to take action. In a set of proposed amendments to its directive on data protection, which forms the basis of data protection laws in member states, including the UK’s Data Protection Act, the EC has developed a new regulation, including measures to protect an individual’s ‘right to be forgotten.’


Designed to harmonise rules across the EU’s 28 member countries – that’s half a billion citizens – this new regulation makes privacy and data protection integral to technological development, organisational processes and structure. The scope of the act will increase significantly as it standardises and unifies data privacy requirements not just across the member states, but for any businesses that markets to the EU, as well as addressing the export of personal data outside the EU.
Coming into force in less than 12 months time, the GDPR is described as the biggest shake-up to privacy regulation for 20 years. It introduces a host of new concepts: appropriate data governance; privacy by design and mandatory Data Protection Impact Assessments (DPIAs). The new regulation holds all parties within the supply chain accountable for assuring the confidentiality and integrity of the personal data being held.

Carrying heavy fines for non-compliance, up to €20 million or 4 per cent of global turnover, whichever is greater, the GDPR endorses stricter guidelines for getting consent for data collection, individual profiling and also contains more comprehensive definitions of data.

The GDPR also enhances the current legislature around data security and breach notification standards, so it is imperative that compliance teams, CIOs and data protection officers take notice of these changes.

The countdown to GDPR has begun.

"GDPR is driving modern data protection strategies"
Chapter 2: The impact of GDPR on people, processes & technology

The European Commission’s General Data Protection Regulation (GDPR) will introduce new and wide-reaching legal obligations relating to how businesses collect, store and share personal information.

This incoming regulation poses several challenges for businesses. Aside from the 72-hour mandate to disclose a breach, the threat of huge fines, the appointment of a data protection officer and ensuring they and their supply chain uphold diligent data management standards, businesses may also have to revise processes around accessibility, retention and deletion of personal data so they are compliant under these stricter data protection rules.

For EU citizens, the new rules mean:

**THE RIGHT TO BE FORGOTTEN:**
Data will be deleted when a consumer says they no longer want their data to be processed providing there are no legitimate grounds for retaining it

**DATA PORTABILITY:**
People will be able to transfer personal data from one service provider to another more easily with the aim of improving competition among services

**EASIER DATA ACCESS:**
Individuals will have access to their own data

**BREACH NOTIFICATION:**
Companies and organisations must notify the Data Protection Authority of serious data breaches and hacks as soon as possible (ideally within 24 hours) so that users can take appropriate measures

The impact of the GDPR on processes

There are far reaching changes in the GDPR, among them demands that data is kept only for as long as it is required and any data kept must be kept in accordance with the GDPR.

The forthcoming act will also be particularly tight around the **right to be forgotten** and **data accessibility**. Effectively, Article 17 of this new regulation, which addresses the ‘right to erasure’ or ‘right to be forgotten’ – coupled with the new ‘right of access’, is likely to impact almost every company in the world.

“GDPR will change the data archiving culture within every business”
Under the GDPR, individuals will have the right to obtain confirmation to how their data is being processed and have access to their personal data. The GDPR even goes so far to recommend that organisations should provide remote access via a secure self-service system, which would provide the individual with direct access to his or her information (Recital 63).

“GDPR will change the backup and recovery strategy within every business”

Understandably, this will not be appropriate for all organisations, but there are some sectors where this may work well. However, every organisation will need to have processes and procedures in place to be able to access and erase personal data held about an individual. Furthermore, it represents a significant challenge to those organisations that back up and store archived copies of personal data on tapes and will effectively force change in the way businesses approach data backup, recovery and archiving when it is enforced in less than twelve months time.

“The data protection world has changed radically over the past 20 years – ‘seeing what you can find’ from backup tapes will no longer suffice”

And you are not alone. Around 49% of businesses still use tape to back up and archive offsite copy as part of their backup and recovery strategy.

We know that the GDPR marks a dramatic change in the way personal data is collected, stored and shared by businesses and failure to prepare will expose your business to the huge financial sanctions that could be enforced under the GDPR.

In this whitepaper, we want to look at the GDPR in a specific light – and one you might not have considered before – backup, accessibility and how to forget people.

“The real purpose of the GDPR is to shift control of personal data back to the owner of that data”
Chapter 3: Backup, accessibility and how to forget people

It sounds like an oxymoron: we retain personal data to remember people, track their relationship to the business and typically invest heavily in CRM systems and integrated business platforms to ensure we create and send the right messages at the right time to the right people. Combined with the Big Data and social media explosions, organisations can now collect more and more personal data from multiple sources to accurately refine the sales process right down to an individualised level.

Data protection laws have been around for a long time. But mistakes do happen. In the last couple of years some high-profile companies (such as Yahoo! and Talk Talk) found failing to address the myriad of security and protection issues can be expensive in terms of remediation, fines and probably the most costly, customer confidence.

It seems the cost of noncompliance wasn’t high enough. But the GDPR will completely change the game.

The right to be forgotten

Perhaps one of the most controversial proposals, and the one that will attract the most general interest, is the right to be forgotten.

This subject has been discussed at data protection conferences in Europe over the years because of both the positive implications it has for the individual, and the practical implications that this right will have for businesses.

Consumers can demand that all traces of them are removed from a company system and this effectively includes any data held on back-up tapes and in data storage systems. And companies can’t refuse, as withdrawing consent is a major new aspect to data protection introduced with the GDPR, and fines are set to rise massively if they don’t comply.
This rule places a great weight on data management. From a data storage technology viewpoint, the biggest impact will be the need to support this by enabling the ‘ability to be found’. It will require organisations to access and locate the data quickly, so discovery capability will become essential.

With 49% of organisations still using backup tapes as part of their backup and recovery strategy, this is not something that many organisations can currently do. This means that organisations may have to consider building new IT systems and putting in place new procedures so that, in future, they will be able to categorise personal data in such a way that this becomes possible.

**A typical scenario - Let’s imagine:**
You follow the 3-2-1 rule when it comes to backups – just like we recommend here at The Bunker. A consumer has just submitted a ‘right to be forgotten’ request to be removed from your stored data – be it your database, your CRM or your accounts system. To remain compliant with the GDPR you must respond quickly, within one month – which is achievable. But what about the old archived copies on tape which still counts as stored data?

**The beginning of the end for tape storage**
The problem with tape is that data does not exist in the same way as it does on disk. It’s not possible to delete a record from a database on a tape. Or even a single file, as tape stores data in blocks written sequentially, and unlike disk it can’t be randomly accessed. You can only wipe the entire tape. And you may very well have hundreds, if not thousands of backup tapes, some you keep onsite in a fireproof safe, but most are safely kept offsite in your disaster recovery location. The target file, or files, that you have been asked to delete can be on any of these backup tapes.

“The EC articulates the right to be forgotten as the right of individuals to have their data no longer processed and deleted when [it is] no longer needed for legitimate purposes”
The “how to forget people” headache - an almost impossible task

How do you find the backup tape that stores your target file?
Your files aren’t actually individually copied to your backup tapes. Your backup tapes store backup images and each image may contain multiple files. This means that you first must identify the backup image that contains your target file before you can determine which backup tape you must retrieve.

How do you delete the target file from the backup tape?
Unfortunately, you cannot selectively destroy a backup image on a backup tape. You have to destroy everything else on that backup tape too. You may have to first duplicate out all the other backup images from the backup tape except for the backup image that contains the target file, and then perform (long) erasure of the backup tape. And if the backup image also contains other files that must be kept, then you first need to restore that backup image, delete the file, and then backup the rest again.

What else could you do?
You could restore the tapes to a test system, pull the database into a copy of the live application, systematically delete the records and then save the data back out to tape. But how many tapes do you have and how long does it take to restore an individual tape? Imagine the strain this would place on already overburdened IT departments.

Retain and repeat
Depending on your data retention policies you could have multiple copies of the data across lots of tapes and will to have to repeat these steps for several more backup tapes, all within 30 days or risk hefty fines. And every time the media features a story reminding people they can be forgotten - especially around the enforcement start date of 25 May 2018 - you can expect a deluge of right to be forgotten requests and the process is on repeat…
The cost of data accessibility

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63). Organisations must provide a copy of the information free of charge – a change for UK companies - and within 30 days. Companies are also expected to verify the identity of the person making the request, using “reasonable means”. If the request is made in electronic form, the information should be provided in a commonly used electronic form. This could impose costs on companies who use special formats, such as tape media or paper records.

Recital 63 also suggests that, where possible, organisations should provide a secure system, which would grant individuals direct access to their data. But in terms of real costs, of getting the business GDPR ready – the removal of fees is only a small part of the picture. How long will it take you to access your customer data, let alone provide secure access to every individual?

Without doubt it’s a time consuming and costly project for those using backup tapes. Just calculate the days taken to find the record, get it customer ready in their requested file format and depending on the type of request, maybe even deleting it, adding on the time to restore and then back it up again, and not forgetting to validate it worked. Then multiply that by the number of tapes you have. And then think about undertaking this process for every potential request for removal under the GDPR and you start to see the magnitude of the problem.

Personal data - the impacted principles:

Article 5 of the GDPR covers a number of principles relating to personal data processing which will pose a number of additional challenges around backups. Article 5 requires that personal data shall be:

- Principle 2 – collected for specific, explicit and legitimate purposes
- Principle 3 – adequate, relevant and limited to the purpose
- Principle 4 – accurate and kept up to date
- Principle 5 – kept in a form which permits identification of data subject no longer than is necessary

For some organisations, trying to remain aligned with these principles – and therefore compliant – is going to require real effort and be a real challenge.
In summary
If your customer evokes their “right of access” or their “right to be forgotten,” then you need to be able to access their data simply and at speed – as there is only one month to respond in order to remain compliant with the GDPR.

Companies need to re-examine how they archive and access their data, including live systems and legacy backups if they are to avoid the potentially business-breaking consequences of legislation post GDPR. It’s a case of adapt or die. The old attitude – ‘we’ve always done it this way’ – simply has to change.

And there’s less than 12 months to go!
Chapter 4: Notification of breach

Another key change to how personal data will be used and processed under the new GDPR framework is the introduction of the breach notification. The GDPR will impose a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected, too. As part of the new framework set by the EU, the GDPR states that all companies have up to 72 hours - where feasible - to provide notification of a breach of EU national’s data.

What could a data breach mean to my business?
As well as this requirement, the regulator will also be able to impose a stratospheric rise in penalties for security breaches. Businesses found to be in breach will be breaking the law and subject to fines of up to €20m or 4% of global turnover, although this does not apply to all breaches. Businesses will have to go public if they are subject to a breach, which is significant given that just 28% of breaches were disclosed last year. The fact is it’s no longer acceptable for firms to keep a breach quiet and hope that nobody finds out. But regulatory fines are only part of the downside for companies, with reputational damage, business disruption and revenue loss also having a significant impact on firms suffering a data breach.

2 tiers of administrative fines:
• Up to €10m or 2% of global turnover, whichever is the greater
• Up to €20m or 4% of global turnover, whichever is the greater
In the UK, firms are not currently under any legal obligation to announce a data breach, with many choosing not to as the cost of doing so for a business can be enormous – as demonstrated when TalkTalk and Carphone Warehouse saw their profits and trust in their brands fall dramatically following public data leaks.

This will be a significant change for many businesses, and will see current systems overhauled in order to ensure breach protocols are compliant with the new legislation. It will also apply to all UK firms trading in Europe, as any company that holds the personal details of an EU ‘data subject’ will have to comply.

**A data breach is more than just losing personal data:**

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- **Confidentiality breach** – unauthorised disclosure of, or access to, personal data
- **Integrity breach** – the alteration of personal data
- **Availability breach** – the accidental or unlawful destruction or loss of personal data

All breaches must be reported within 72 hours

**Fast Facts**

- UK businesses could face up to £122bn in penalties for data breaches when new EU legislation comes into effect in 2018
- According to a UK government 2015 information security breaches survey, 90% of large organisations and 74% of SMEs reported a security breach, leading to an estimated total of £1.4bn in regulatory fines


“The stratospheric fines of non-compliance will be an absolute game-changer for both large corporates and SMEs”
In the News

Behind the sensationalist headlines of the recent Ransomware attack on the UK’s National Health Service, is the inconvenient truth that on this occasion much of the disruption could have been avoided. The attack on the NHS not only highlights the dangers of having critical infrastructure running on legacy technology, but also shows how quickly personal – and in this a case life threatening – data can be accessed. If such an event reoccurs after 25 May 2018, the fines would be astronomical – and it’s not clear who’s purse would be paying the penalty.

In summary:
Make no mistake; the EU’s GDPR is a real game changer. Firms that underestimate its implications do so at great peril.

If you are breached, if something goes wrong and you lose data, you will be investigated under the powers of the GDPR. If it can be proven that you haven’t behaved appropriately and have failed to put in the correct or state of the art measures to control your data, you will be subject to the full force of EU law.
Chapter 5: How to get GDPR ready

With less than 12 months to get GDPR ready, every organisation, large and small, needs to become compliant and simplify the “ability to be found.” If organisations don’t change the way they backup and archive data, they will find the new rules overwhelmingly complex. You need to act now.

To address the data recovery, archiving and backup challenges discussed in this paper, one solution to this is to move to an online cloud based backup solution that allows the rapid retrieval of data without physical tape media in the mix.

The advantages of cloud over tape

Traditional methods of backing up large amounts of valuable data, such as tape backups and offline storage, are becoming less cost effective and increasingly time consuming.

Cloud technology changes this. Cloud archiving includes all of the replica charges, which would typically triple that tape media cost. Cloud removes the need and subsequent cost and storage of an offsite tape library, is completely hands-free and can be automated, so labour costs are instantly removed. For large libraries, this dwarfs the media cost, making the cloud approach economically very attractive. Cloud archives can also be accessed in seconds and each item of data can be located fast.

This has a major impact on the real purpose of archiving and backup, which is to get the data back quickly when local copies are lost or a disaster occurs – and moreover, it fits perfectly in line with the new GDPR directives and its 30 day response rate to fulfill a right to be forgotten request.

Backup as a Service - Powered by Veeam

As the GDPR enforcement date looms, we have developed an innovative, ultra secure, cloud-based backup solution.

Powered by Veeam, The Bunker’s Backup as a Service (BaaS) is an ultra secure cloud backup solution that efficiently maintains offsite copies of your backups, along with the ability of restoring them in time of need. It provides a simple-to-use client interface, unlimited scalability, 24/7/365 dedicated technical support from our specialist technicians trained in data backup and recovery along with flexible storage in our ultra secure UK-based data centres.

Available on-demand, our BaaS is an ultra-secure, reliable, cost efficient, comprehensive and compliant method of backing up your critical data. Available as a managed or unmanaged service, and with a large range of additional options, you can build your own bespoke secure cloud backup and recovery service to fit your exact business needs.
The benefits of BaaS

• Reduced tape costs for management, transportation and storage
• Access and locate data quickly, simplifying the ability to be found
• Data readily available and secure
• Cheaper and faster backups
• Reduced storage costs through 90%-95% (or even higher) data de-duplication ratios and cost-per-terabyte licensing
• Boost in backup performance ensures that backups complete within the backup window and improves backup success rates
• Significant reduction in backup administration time frees staff for higher value tasks
• Reduced support calls; platform reliability and stability makes 24×7 support easy to deliver

In summary:
The bottom line is that for most users, we’ve reached the point where tape’s advantage over storage on disk has been succeeded by the cloud’s advantage over tape.

Our cloud-based backup solution can be seen as a direct replacement for tape and is easier than you think to deploy. Additionally, it also contributes to a strategy that will help protect you from ransomware, human error, server theft or failure.

The Bunker has over a decade of experience in deploying compliant, secure systems. Over the years, we have built the necessary methodologies that help meet the most rigorous of standards and compliance regulations.

The GDPR will change the data management culture for businesses. And The Bunker is well prepared. Our continual assurance approach ensures our customers remain fully compliant, mitigate risk and remain ultra-secure, with our transparent, auditable and diligent IT processes to guarantee data protection requirements are met.

Along with our own experienced, in-house Data Protection Officer, we can work with you to help prepare for these changes and take the necessary steps towards ensuring full GDPR compliance.
Conclusion

GDPR comes into force on 25 May 2018.

There are just under 12 months and in turn one budget cycle remaining until the law enforces the act, yet GDPR readiness is not a priority amongst IT professionals in Europe. And according to DMA, 26 percent of marketers believe their businesses are unprepared for the GDPR, and just two thirds (68 percent) believe they will be compliant in time for the May 2018 deadline.

However, based on our extensive experience, we expect to see businesses eliminating tape as 2017 continues, as more and more turn to the cloud to backup for long-term data retention. This will be driven by improving cloud storage economics, increased confidence in data security and the maturing of de-dupe-to-the-cloud technologies – and of course by the GDPR.

Multiple Initiatives to drive GDPR Compliance

To comply with the GDPR, businesses will need to be able to answer four challenging questions:

1. Do you have visibility and insight into the personal data you store?
2. Can you locate all of the information you hold on a data subject?
3. Can you supply that data to a requestor within a tight deadline?
4. Can you prove what you’re doing with that data and is it protected?

The ability to answer these questions will force firms to embark on a long overdue data management journey, which in turn will result in additional benefits in terms of reduced data storage and management costs.

Looking forward

There is a lot to assess in that time, so now is the time to be getting systems ready for compliance and for implementing new breach notification policies. This will require working with legal teams and other branches of the business to ensure compliance is watertight to prevent heavy fines for businesses.

It’s time to go tapeless

Organisations who only backup to tape - making it almost impossible (or at least very expensive) to furnish a “right to be forgotten” request - will need to address their data management policies sooner rather than later. And not just because of the GDPR, the challenge to respond to a right to be forgotten request and the risk hefty fines: Savvy business should use this opportunity to shift away from tape and embrace the additional positive business benefits of a tapeless world which are all well documented in this paper.

Brexit doesn’t change anything

And as a brief, final and crucial aside, the GDPR will affect UK based companies regardless of the UK’s impending exit from the EU – as the UK is adopting GDPR before we leave and impacts any firm handling any EU citizens’ personal data.
In summary
There is likely to be a difference between what is currently proposed by the new framework and what the actual regulations will look like in one years' time when finally implemented.

Whether the structural changes or some of the obligations, such as the right to be forgotten, will be altered, who knows? We can only wait and see.

What we do know is that this new framework will mark a noticeable change in how organisations process personal data. The potential financial penalties should help to focus the mind of those organisations that have been putting data protection compliance low on their list of priorities.