Executive Insight Paper

In association with

GDPR: the Security Dimension

Information security, governance and regulation in harmony

Freeform Dynamics, 2018

In a nutshell

About this Document

The insights presented in this document are derived from ongoing independent research, coupled with specific briefings from CA Technologies on their security offerings. While specific technologies are used to illustrate how key generic principles translate to practical reality, nothing in this paper should be taken as a validation or endorsement of any product or supplier.

The EU's General Data Protection Regulation (GDPR) is reshaping the way that organizations need to think about data security, as well as driving them towards better information governance. That's because data security is implicit to GDPR – after all, without security, data cannot be private.

And privacy is what the GDPR is all about – a privacy that encompasses control of how, as an individual, your personal data is collected, stored and used. For some organizations, this will require a significant shift in their mindset. It will force them to recognize that the personal data which they have painstakingly collected is not theirs to do with as they wish. Under GDPR, our personal data is ours – the organizations we share it with are its guardians or stewards, not its owners, and they must guard and use it in a trustworthy manner.

Clearly, IT security professionals have a major role to play in all of this. Our aim with this document is not to provide a comprehensive guide to GDPR compliance. Rather, we will highlight areas of interest and concern to security professionals – some key aspects of GDPR that you will need to investigate further to ensure that your GDPR planning is fully aligned with your organization's operational plans.

We will go on to discuss examples of how security software, such as that provided by CA Technologies, can address the technical elements of GDPR compliance, and how that in turn can provide a foundation on which to build the essential processes and policies that actually make an organization compliant.

The vital role of IT security in GDPR

GDPR is reshaping the way organizations must think about personal data privacy.

Much has been written about the GDPR, what it means for our personal data, which organizations and operational functions it affects and how they should respond to it. Marketing and data protection aspects have received a lot of attention, because GDPR will bring significant changes to how those areas work from day to day.

The role of the IT security professional in GDPR compliance has rarely been accorded the importance it deserves, however. For the security pro, GDPR is not just a matter of new and changed tasks at work – although it will bring those. The fact is that IT security professionals, departments and software vendors are essential to GDPR compliance.

Indeed, they are in some ways its bedrock, because information security is implicit to GDPR. After all, without security and all the things that flow from it, such as identity management, anti-malware defenses, access control, data loss prevention, and probably encryption too, personal data cannot reliably be kept private.

Information security is implicit to GDPR: without it, personal data cannot reliably be kept private.

The GDPR outlined

The fundamental precepts of GDPR can be summed up relatively simply:

- People are the owners of their personal data and retain control over it
- Organizations are its stewards or guardians, not its owners
- As the steward of personal data, you must protect it appropriately, and
- You can only use the data you steward in ways for which you have a lawful reason.

Much of the GDPR is descriptive rather than prescriptive – it tells you what should happen, not how to it.

Of course, there is a lot of important underlying detail to understand too, and there are a number of significant caveats and cautions. In addition, much of the GDPR text is descriptive rather than prescriptive – that is, it tells you what should happen, not how to do it – and it has yet to be tested in court. However, adopting a mindset based around the points above should help a great deal when it comes to working through the detail and seeing how it will affect your organization.

And we could perhaps add a fifth item as a corollary, which is that good information governance and security is also good for business. It might seem like a chore, or unnecessary red tape, but organizations today are collecting and creating data faster and in larger quantities than ever before. The downside of that data growth is that it gets even harder to manage that data and gain business value from it. At the same time, if you also lack good information governance and security then the risks of data breaches, or of damaging the organization's reputation and business in other ways, are growing fast as well.

Software tools can help, as can the likes of ISO 27001.

Fortunately, there are more software tools than ever before, at lower costs, to help organizations do a better job of information management. There are also standards to help with best practices in information governance and security, notably ISO 27001, which we will briefly discuss later.

Some GDPR specifics

A full consideration of the regulation is a matter for your organization's data protection officer or data controller. However, here are some of the highlights most relevant to IT and information security.

Subject rights

GDPR gives people considerable rights over their personal data and its privacy.

Perhaps the most obvious change arising from the GDPR is that it conveys new rights to data subjects – the 'natural persons' whose data an organization might collect. These include the rights to:

- Erasure, to be forgotten or deleted from the database, unless there is an overriding legal or regulatory requirement to keep that data
- Access and rectification, seeing and if necessary fixing the personal data held on file
- Restriction of processing, where the subject has legitimate grounds to object, but for other reasons their data is not to be deleted
- Data portability, exporting data in a machine-readable format.

These rights will be new to many organizations, and they will need to add support for them to their systems and work processes. Needless to say, they will also require comprehensive information security provisions.

Informed consent

Consent to the processing of personal data must be both explicit and informed.

For some processing activities, you will need unambiguous and affirmative consent from the data subject. Affirmative means they must actively opt-in or agree – conditional agreements ("By placing this order you agree to"), or where the default is to agree and they must actively opt-out by unticking a box, do not constitute consent. This consent must also be adequately informed, with a clear explanation of what they are agreeing to and who the agreement is with.

Other lawful reasons

There are other lawful reasons for processing personal data besides consent.

Consent is not the only lawful basis for processing personal data, however. Obvious commercial alternatives include performance of a contract – collecting a customer's name and address so you can deliver their goods does not need additional consent, for example. Other potentially lawful reasons include fraud detection, monitoring public health, fulfilling legal obligations, and historical or scientific archiving.

Data minimization

The principle that you do not collect more personal data than you need is a matter of respect and good governance. However, it may have been ignored in the past, with departments collecting as much data as possible "just in case it is useful in the future". This will no longer be permissible, and organizations will also need to review the personal data they already hold, with an attitude of "If we don't need it, don't keep it".

State of the art

Keeping your security up to date is essential to stay compliant.

An essential consideration is that GDPR compliance is not static. For example, it requires you to implement all necessary security and integrity measures to ensure that data is protected, kept confidential, and is not inappropriately modified. But this is not a 'fit and forget' process – several provisions within the regulation mention the state of the art, clearly implying that you can only remain compliant if you keep your IT security up to date.

Personal data

This is every piece of data that can be used to uniquely identify a person, or data that is about an already identified person. It can be data that the user has explicitly provided, but it can also be data that you have collected about them from third parties, say, or from their activity on your website or your app.

Sensitive personal data

Sensitive personal data requires extra security.

This is a subset that requires additional protection. It includes data that might reveal the subject's ethnic origin, political opinions or sexual orientation, for example, as well as biometric data that uniquely identifies them.

Pseudonymization

A term that crops up several times within the regulation, pseudonymization separates the data from the personal identifiers, which are held in a separate database and linked by keys such as random identity numbers. Because the process can be reversed, either legitimately or perhaps by an attacker stealing the key or combining your data with third-party data, the data is not anonymous.

Pseudonymized data can reduce the security risk, but is still regulated by GDPR.

This is important because pseudonymous data is still regulated by the GDPR, whereas truly anonymous data is not. The advantage of pseudonymization is that it can reduce the security risk while maintaining the data's utility. Again, this is an area where you must keep up with the state of the art. If someone develops a way to break your pseudonymization, then your data can no longer be considered safe.

That said, it is important to recognize that pseudonymization is entirely optional. It is one way for an organization to enhance the security of the personal data it holds, and

it may allow data to be processed for a purpose other than the one it was collected for, but it is neither mandatory nor sufficient security on its own.

The only exemptions are personal or household activities, national security and law enforcement.

Exemptions

Purely personal or household activities are exempt – a family address book, perhaps – as are national security and law enforcement authorities. Additionally, organizations with fewer than 250 employees have a lighter record-keeping burden, and the rules are different for public authorities and bodies. But in essence, if you offer services or goods to EU residents, monitor the behavior of people within the EU, or control personal data within the EU, then you must comply with the GDPR.

Building the GDPR-fit enterprise

GDPR compliance is a matter of understanding your data, then having the right policies and procedures in place, and making sure that they are adhered to. However, this is not something that can easily be built on manual processes. This is especially true when we look at GDPR through the lens of security.

Security skills and software are essential to create the solid foundation on which you can build the policies and processes needed for GDPR compliance.

In this section then, we will look at how one might build the security foundations necessary for GDPR compliance, taking as our example one of the major vendors of security software. In the interests of full disclosure, we are using CA Technologies, as they are sponsoring this paper. CA Technologies is not the only vendor of security software, however, and its inclusion here should not be construed as Freeform Dynamics endorsing any particular offering. That said, CA is one of the few organizations that covers the gamut of data processing systems from mainframes to distributed systems.

The requirements of GDPR, and what you need to implement in order to be compliant, fall into four broad themes or subject areas. These then thread through the day-to-day operational and security functions, as we will discuss below. The four key themes are:

- Privacy & procedural controls
- Data subject rights
- Auditing & reporting
- Breach assessment & notification.

Privacy & procedural controls

Examine your existing data collection processes and storage workflows to ensure they become – or remain – compliant in the future.

These are the essential processes, policies and systems to ensure that access to personal data is properly regulated. Part of the procedures and processes aspect is to ensure that all teams in the organization are 'on the same page'. For example, security must work with all the other relevant teams to examine the organization's existing processes for data collection and storage, and to assess and understand its policies for processing and its storage workflows. This is both to check that they are compliant now, and to ensure they remain or become compliant in the future.

Data discovery and classification

This is likely to be the starting point for any compliance project, because you can't control access without understanding what personal and sensitive data you hold,

where it is stored, and what regulations it is subject to. This includes test, backup and archive copies, and data synched to a mobile device or to cloud storage, of course.

Automating the process of discovering stored personal data, even when it has been hidden, lost or abandoned, and classifying it according to its level of sensitivity, is where tools like CA Data Content Discovery, CA Compliance Event Manager (for mainframe data) and CA Data Protection could come in.

Strong identity governance and access control is vital to minimize entitlement creep, privilege escalation and credential misuse.

Cohesive identity and access governance

Coming back to the basics of privacy, you don't just need to know who should have access to the data and who has actually accessed it, you also need to know who has access to it but should not have – entitlement creep and privilege escalation are well known problems within access control structures. That requires strong identity governance policies, based on identity management software that supports role-based provisioning, management of access requests, enforcement of least-privilege controls, and automated de-provisioning when staff leave or change roles.

User access control is essential here. Not only do you need to know who is authorized to access what (ideally with least-privilege controls in place), you also need to know who accessed what, and when. Similarly, cohesive identity management will make it much easier to map privileges and flag dubious behavior, compared to having access controls fragmented by application.

Enforcing access policies intelligently is where technology like CA Identity Suite comes in. Then tools such as CA Privileged Access Management (PAM), CA PAM Server Control, and CA Trusted Access Manager for Z can add the ability to deploy, manage and monitor privileged user policies. They can also help to defend those privileged accounts, supporting strong authentication and securing server and storage resources to prevent lateral movement of data.

Single sign-on can aid security reporting, as well as easing user access.

A useful addition here is software along the lines of CA Single Sign-On. Not only can the solution help simplify access management, but it also contributes to the auditing and reporting requirement because it identifies the device being used.

Privacy by design

Privacy by design has always been good practice, but the GDPR gives it a degree of regulatory force. It is the principle that data protection and privacy is designed into your applications, systems and processes from the outset, not added as an afterthought. Data minimization and encryption are among the techniques that can contribute towards privacy by design.

Pseudonymization

Removing indirect identifiers, as well as direct identifiers, is a notable security and identity challenge.

This is a very useful GDPR option, but one that is potentially complex to implement, thanks to the need to ensure that indirect identifiers are also removed or obscured along with direct identifiers. Fortunately, it is also one that has heritage within areas such as software testing, which is why mature identity and data protection suites can have important roles to play, alongside more specific solutions such as CA Test Data Management.

Data subject rights

Data subject rights must be integrated into your systems and apps, too.

Providing external users with access to personal data might seem to contradict the security principles within GDPR, but it may be the most manageable way to meet the rights that data subjects have to access their own data – given effective identity management and suitably strong authentication, of course. For many organizations, this will be the biggest innovation or change needed for GDPR compliance.

Any software that contributes to data protection and access control also has a role to play here – not too surprisingly, given that what data subjects need is essentially a restricted form of privileged access.

You will also need to integrate those rights into your systems and apps – for example, to remove restricted data from processing or support data rectification. These functions can be assisted using solutions along the lines of the CA API Management toolkit and its peers.

Consent management

This is closely related and is another innovation that GDPR requires. Of course, consent is not the only lawful basis for processing personal data, as discussed earlier, but it is arguably the one that requires the most care in implementation. This is because as well as giving consent, data subjects can withdraw or restrict it, and this must be securely reflected in the data and the operational processes.

Auditing & reporting

Demonstrating your compliance is as important as compliance itself.

Data controllers and processors need to be able to verify compliance, but auditing has other potential uses too. For example, as part of the discovery process it can help establish the ownership of data. Similarly, advanced auditing tools can also warn of exceptions that may indicate security and/or compliance breaches.

It is useful to remember in all this that demonstrating compliance is as important as compliance itself. Indeed, if you are not yet compliant, it is vital to be able to show the steps you are taking towards compliance, as these can be offered in mitigation should you suffer a breach or other default.

Another significant step in this area is to conduct a Privacy Impact Assessment (PIA). This is useful both as a demonstration of compliance (or how close you are to it), and to assist with planning for the future. It also helps to answer the vital question: Are we as secure as we think we are? And in every domain? After all, it only takes one weak link for the chain of trust and compliance to fail.

Cross-border transfer

Data will probably need to be cleaned up before it can safely be moved across organizational or national borders.

As well as removing the borders to information flow within the EU, the GDPR permits personal data transfers to other countries whose legal and regulatory regime provides equivalent privacy protection. However, many corporate mainframes and data centers serve multiple countries, and there is a risk of excessive data and credentials crossing borders, especially within security databases.

It is therefore a good plan to build automated processes to remove redundant or excessive access rights, using the likes of CA Data Protection, CA Identity Suite and CA Cleanup.

Binding corporate rules

These elements of GDPR carry similar risks to cross-border transfers, but apply to data moving within an organization or group of organizations working together. Similar measures are therefore advisable to avoid transferring excessive data or access rights.

Certifications and seals

GDPR compliance monitoring must adapt to the needs of the various corporate officers involved in the process.

As mentioned, the GDPR requires organizations not just to comply, but to be able to demonstrate and certify compliance – and to have the procedures and processes in place to maintain that compliance as their collection, storage and use of personal data evolves. Working with spreadsheets is very unlikely to provide the sort of repeatable traceability and reporting that compliance – and more importantly, the ability to certify compliance – will require. That means you need tools to help manage the process and orchestrate the necessary collaboration.

Ideally, this should all come together on monitoring screens that give the relevant people within the organization, such as the CISO, CFO and data protection officer, access to all the GDPR and compliance-related information and controls they need, presented in a way that is easy and fast to understand. The ability to pull all these functions together and generate KPIs (key performance indicators) can be extremely powerful.

Breach assessment & notification

Breach notifications should say who is affected, what the likely consequences are, and what steps are being taken to mitigate the damage.

Not only must you report a personal data breach within 72 hours of becoming aware of it – where feasible – but the report should contain details of who was affected (the data subjects), what was stolen or lost (the data records), the likely consequences, the measures taken or proposed to deal with the breach – and where possible, the measures to mitigate its adverse effects.

The GDPR breach notification requirements resemble those already in force in the U.S. in some respects. Most notably, there is no need to notify if the data was unidentifiable, thanks, for example, to encryption or anonymization. Overall though, the GDPR requirements are stronger, because they are concerned with privacy per se, and not simply with the risk of fraud or identity theft.

Not too surprisingly, this maps to the same toolset as data protection & assessment, where tools like CA Identity Suite and CA PAM include the necessary auditing, alerting and remediation capabilities for security and compliance violations. On the mainframe, systems such as CA Compliance Event Manager and its peers can act as a SIEM (security information and event management) to provide additional security insight and forensics.

Keeping all the above up to date

GDPR compliance is a living process that must evolve with the organization.

Just like security, GDPR compliance is an ongoing process. This might seem obvious to security professionals, who are used to working in a threat environment that is constantly evolving and becoming more dangerous. However, there are people in every organization whose initial assumption will be that GDPR is yet another box-ticking exercise that can be forgotten as soon as the paperwork has been filed – forgotten until the next audit, at least.

In truth, unless processes and policies are kept up to date, the organization is unlikely to remain compliant. Not only do the risks change, but new data is constantly being collected and a smart organization will want to process it in new ways, some of which may require new explicit consent. At the same time, the technologies and techniques available for data security are constantly evolving, of course, and as the GDPR says, keeping up with the state of the art is essential.

If you are compliant with existing laws and regulations, you should also be a long way towards GDPR compliance.

This is all 'Just good practice'

A key message when discussing GDPR compliance is that, with a few exceptions in areas such as record-keeping and data subject rights, these are all things that a well-governed organization should be doing anyway. Indeed, if you are already compliant with existing laws, directives and regulations around data protection, breach notification and so on – and just as importantly, you can demonstrate that – then you should also be a long way towards GDPR compliance.

Other security resources to support GDPR

Assuming you are already running a secure ship that complies with all the relevant laws and regulations, then a considerable proportion of your existing tooling, skills, policies and processes should be re-usable for GDPR. Here are some of the security resources that may need to be strengthened to assist with GDPR compliance, or which should be strongly considered if they are not already in place.

Ensure that your users are educated about security threats, and that endpoints are properly secured.

Threat protection is essential for GDPR compliance, because any gap in coverage could lead to a data breach. Among other things, this might mean multi-factor authentication, minimized privileges, training and technology to minimize the risk of infection or of stolen credentials via malware and phishing, and the blocking of consumer-grade cloud storage.

Endpoint security is another essential. Several of the high-profile data breaches that involved lost or stolen laptops could have been prevented by proper endpoint security. That means enforcing local data encryption, strong authentication, and keeping the system and security software up to date, for example.

SIEM: If you are hacked, can you not only detect the fact, but also determine which systems were compromised and what data was accessed? This typically requires threat intelligence systems such as SIEM tools, because in anything beyond the most basic of IT systems, there is simply too much data in the log files to sift through it manually. One key aspect here is that any SIEM setup must be physically and logically separated from your main systems, to make it harder for an intruder to compromise or delete the evidence in the log files.

ISO 27001 is a useful step towards GDPR compliance because it is prescriptive, not merely descriptive.

ISO 27001: If you have already implemented the ISO 27001 standard for information protection, you should already have much of GDPR covered. It does not cover all of it though, and it is possible that personal data was not included in your ISO 27001 implementation, perhaps because it was not relevant at that time. Fortunately, you can add the relevant policies subsequently.

Data leakage prevention, or DLP, is technology that watches for personal information and other sensitive data leaving your organization. In some cases, you might want DLP to block the leak, while in others the appropriate response might be to encrypt it and send it on its way.

Switch on encryption wherever and whenever you can.

Encryption is not mandatory, but in practical terms it is essential to GDPR compliance. It covers both encryption of data at rest, whether in your data centre, on a cloud service, on a mobile device or wherever else, and encryption of data in motion – including data in email, on USB sticks, and so on.

Conclusion

As its full name implies, the GDPR is all about protecting data. However, amid all the attention paid to how compliance affects the operational side of the business – sales, marketing, website and app design, data storage and so on – it is also essential to understand the relevance of IT security skills, processes and technologies.

Strong IT security is essential to GDPR compliance, and data privacy will be key to many security risks going forward.

Indeed, unless security professionals make sure that the foundations are solid, with all the software and other technology needed to support the necessary policies and procedures, GDPR compliance cannot be guaranteed. Security pros are also well placed to understand the new risks and challenges that personal data protection and data privacy brings.

This in turn means that security pros must understand what's needed for GDPR compliance, both now and on a continuing basis, and they must participate fully in the continual process of ensuring that.

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we aim to help busy IT and business professionals get up to speed on the latest technology developments, and make better-informed investment decisions.

For more information, and access to our library of free research, please visit www.freeformdynamics.com or follow us on Twitter @FreeformCentral.

About CA

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact, and communicate—across mobile, private, and public cloud, distributed and mainframe environments.

Learn more at www.ca.com.

Terms of Use