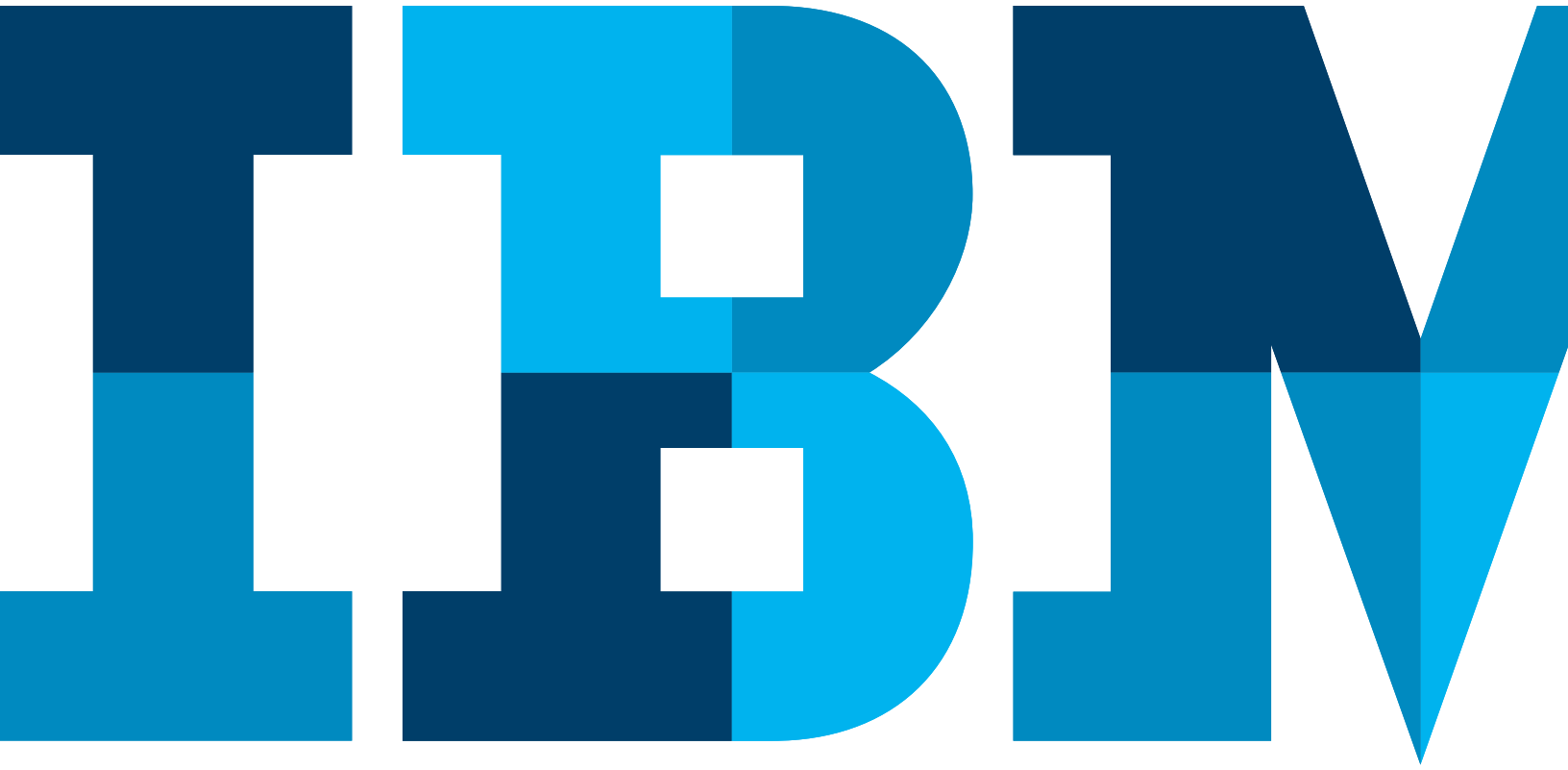
IBM
White Paper

IBM Pathways for GDPR readiness

Preparing your business for the changing realities of data privacy and protection in the EU



IBM

Contents

Introduction

If your organisation carries out business in the European Union, then you may be aware that your life is about to become a lot more complicated starting in May 2018. That's when the new EU General Data Protection Regulation (GDPR) will take effect. IBM is positioned to help you develop strategies to address the challenges of the GDPR. Our Pathways for GDPR readiness are phased programme engagement points and cognitive capabilities which can accelerate your journey.

This new, stronger regulation will aim to harmonise data protection across all 28 EU Member States. In some cases, it will merely strengthen or enhance specific rights which are already in place under many local data privacy laws, whilst other rights and obligations will be introduced for the first time.

The EU has more than 700 million residents and 26 million active businesses which will be impacted directly by the GDPR. In addition, much of the regulation is expected to apply to the data of individuals from the EEA (but non-EU) member states — Norway, Iceland and Liechtenstein — as these countries will likely standardise on many of the same rules included in the GDPR, once it is incorporated into the 1992 EEA Agreement. (It is currently adopted under scrutiny by the EEA EFTA.[1])

Adding to the complexity is the fact that the GDPR is explicitly stated to be extraterritorial in certain broad circumstances. This means that organisations without a physical market presence in the EU will still be required to comply with the GDPR if the following conditions apply:

- The organisation offers paid or unpaid goods or services to individuals located in the EU
- The organisation is monitoring the behaviour of individuals within the EU

In addition, if you work with suppliers or partners that operate in the EU, they will most likely expect you to comply with the GDPR in order to limit their own risk. Simply put, GDPR compliance will soon be considered a requirement to conduct business in Europe.

IBM views the GDPR as a competitive business opportunity, as it may inspire enterprises to adopt unified information governance as part of their core strategy. Unified governance can provide the foundation for success in the digital age. It can be the framework to transform a business by providing insights about what data the business has, where the data is stored, how the data can be used to maximise value and minimise risk, and how to handle the data in a manner that can build trust with individuals.

IBM's GDPR readiness journey

IBM has established and is executing a global programme to prepare for the GDPR, both for our internal processes and for our commercial offerings. IBM recognises that our customers will look to IBM's offerings and technical assistance to help prepare and assist GDPR readiness within their own organisations, and IBM is well-positioned to help meet this critical need. As part of our own GDPR programme, we're enhancing our ongoing commitment to privacy by design, to help ensure that personal data use is limited by default to what is specifically required.

What are the potential drawbacks of failing to comply with GDPR?

The financial penalties for failing to comply with the GDPR are clearly defined: for each instance of noncompliance, your organisation could face a fine of up to 20 million euros or 4 per cent of worldwide annual turnover (revenue), whichever is higher. Of course, this may also result in damage to your brand reputation in the eyes of your customers and employees.

This might even lead you to lose European market share to competitors that have done a better job of preparing themselves. Some IBM clients are already positioning their GDPR readiness as a competitive advantage. By proactively implementing data privacy and security measures, these organisations are poised to potentially improve their reputation. This can provide a valuable selling point to help bring in new clients.

The regulation formally entered into force on 25 May 2016 and we are now in the transitional period before it applies. Companies should not assume they will be allowed a grace period after the regulation applies from 25 May 2018. Indeed, the Information Commissioner's Office (ICO) in the UK has confirmed that noncompliant organisations risk being fined immediately. However, they have also stated they will take a common-sense, pragmatic approach to regulatory principles, expecting organisations to account for what they have done to prepare.[2]

In addition, regulators have powers under the GDPR to potentially disrupt ongoing business if they suspect your organisation might not be conforming with the GDPR. Such an investigation might lead to findings that show you are even further away from being compliant than the regulator — or even you yourself — originally thought.

What's involved with GDPR readiness?

The GDPR is a much more stringent regulation than many in the United States are accustomed to. Many organisations have long looked at data solely as a market resource. The GDPR challenges them to start looking at personal data use as a fundamental human rights issue instead. It includes data privacy, data security and data governance, so any readiness strategy you put into place must address all three of these issues appropriately in order to be effective.

If you consider the pervasive themes in the GDPR, it becomes clear that a GDPR readiness strategy should span people, processes and technology. Many organisations will be able to preserve some of the processes they already have, whilst building on them to fill in any gaps that might exist.

When appropriately implemented, a holistic governance strategy can help you comply with the GDPR, as well as put you in a stronger position to support your other data obligations that might apply to your business.

Five main concepts of GDPR readiness

From our perspective, there are five main concepts organisations should be aware of when it comes to understanding their GDPR obligations:

1. Rights of EU Data Subjects
2. Security of Processing
3. Lawfulness and Consent
4. Accountability of Compliance
5. Design and Default

Key Duties, Obligations and Sanctions

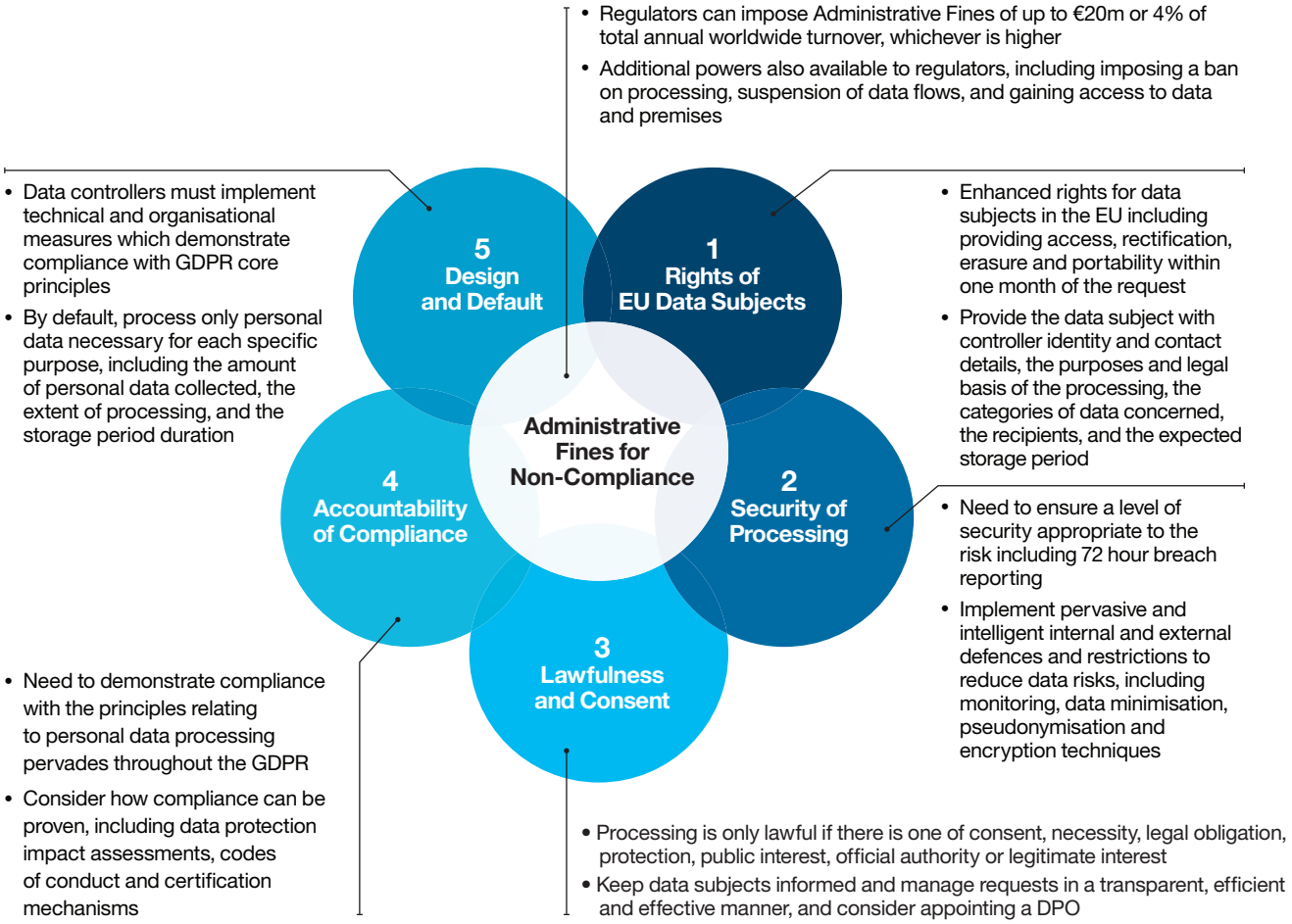


Figure 1: From the IBM perspective, there are five main concepts when it comes to understanding your GDPR obligations.

1. Rights of EU Data Subjects

Rights that will apply to all data subjects in the appropriate circumstances include rights to information, access, rectification, erasure, restriction of processing, portability and objection. Your organisation will also be required to make it easy for customers to understand what their rights are when it comes to their personal data, and to comply within 30 days of receipt[3] to any rights requests they might make.

One important step you can take to help meet these requirements is to maintain data quality. Identifying redundant, obsolete and trivial (ROT) data and disposing of it promptly can help you reduce costs and risks, in addition to helping with your GDPR readiness. Any data that remains once you have done this should be kept readily available in a usable format across both structured and unstructured data sources; this is subject to your responsibilities under GDPR principles such as data minimisation and storage limitations.

2. Security of Processing

Your organisation must provide a level of data security that is appropriate to the risks you face. One requirement of the GDPR is for the controller, when appropriate, to report personal data breaches to the regulator within a 72-hour window and to the data subject without undue delay after becoming aware of the breach. As a result, you would benefit from implementing data security tools that support a rapid response, which may also help you minimise reputational damage.

It is also helpful to consider pre-incident measures that could prevent a damaging personal data breach from occurring in the first place. Techniques you could utilise to accomplish these measures that are specifically mentioned in the GDPR include minimisation, pseudonymisation and encryption. Although not a panacea, encrypting data could remove the need for you to notify data subjects in the aftermath of a personal data breach, although the duty to notify the regulator would remain.

3. Lawfulness and Consent

Under the terms of the GDPR, processing of personal data is only allowed if there is a lawful basis for such processing. One such lawful basis is the consent of the data subject to such processing. Ensuring you have such consent of data subjects before processing their data will likely become much more difficult than it has been in the past. In order for consent to be considered valid, it must be freely given, specific, informed, and unambiguous. In cases such as healthcare, where special categories of personal data are more likely to be handled, it must also be explicit. Complicating issues further, consent can be withdrawn by the data subject at any time.

Whatever process you use to obtain consent from data subjects, it must be done in a manner that is mindful of the other lawful reasons for processing personal data (such as to fulfil a contract or a government requirement). Consent must also be gained with complete transparency. In order to address all of these issues, your organisation should consider adopting a consent management system, supported by activities which could be considered best practices, including implementing workflow tracking and instituting a single source of truth about the data.

In addition to consent, there are other possible legal bases legitimising the processing of personal data, including contractual necessity and legitimate interest. For this reason, it is very important that you know exactly what data you have, the purposes of processing such data, and what you are permitted to do with it. Data mapping and data discovery are important steps your organisation can take to gain these insights, with the end goal being to have a complete understanding of the personal data being processed. In addition, seeking appropriate legal advice and designating a data protection officer (DPO), as will be required under the GDPR for many organisations, can be helpful. Finally, utilise the ongoing "*Article 29 Working Party*" publications to get the latest guidance and interpretations directly from the regulators.[4]

4. Accountability of Compliance

It is not enough for your organisation simply to work toward GDPR compliance. You must also be able to demonstrate your compliance, or document how you are progressing toward compliance. Steps to take to help accomplish this goal include conducting risk assessments, including data protection impact assessments, establishing a governance organisation with roles and responsibilities, implementing a system of recordkeeping that formalises data protection, and creating enterprise-wise codes of conduct, procedures and policies.

Article 30 of the GDPR covers records of processing activities, which are generally recognised as a form of data mapping specific to the GDPR and can help with your organisation's accountability. These records should be managed in a proactive manner with appropriate tooling, avoiding static and siloed spreadsheets if possible. These tend only to offer limited insight and can quickly become outdated. You can safely assume this record of processing will be one of the first things any regulator requests after arriving at your organisation.

Effective management of your controller/ processor relationship is a critical part of data mapping and overall GDPR compliance. The design of appropriate technical and organisational measures (TOMs), audit practices and overall vendor governance should be key focus areas for your organisation.

5. Design and Default

When considering the design element, the principle of privacy by design is specifically mentioned as part of the integration of necessary safeguards into processing, to help protect the rights of data subjects and conform with the GDPR. Similarly, when considering the default element, only the required amount of personal data necessary for the specific purposes of a processing activity should be collected or stored and only for the needed time period. Under the regulation, consideration is given to this data throughout its lifecycle, from collection to disposition, with a particular focus on limiting access to individuals only for the intended purpose.

The IBM GDPR Framework

IBM has created a GDPR Framework that highlights five phases to help achieve readiness, as shown in Figure 2: Assess, Design, Transform, Operate and Conform. The goal of the framework is to translate GDPR obligations into actions and outcomes that help clients effectively manage both security and privacy, to help reduce risk and avoid incidents.

Pathways for pursuing GDPR readiness

Many organisations are aware they need to take action now in order to prepare for the GDPR but are not sure of the best way to get started. The truth is there is no one right answer: where you start depends a lot on where you are now. That being said, IBM has examined our existing client engagements as well as our own IBM readiness initiatives, and identified several common Pathways within the GDPR framework that are the highest priority for most organisations facing the immediate challenges of GDPR readiness. In addition, we have developed various other Pathways that companies might want to address in the future. Figure 3 illustrates the major pathways within the IBM GDPR framework.

GDPR Pathways for immediate attention

Assess: GDPR readiness assessment

If you haven't already done so, your first step should be to understand your GDPR obligations and state of readiness, as well as the risks of failing to act now.

A key outcome of this GDPR readiness assessment should be a roadmap that helps you manage and mitigate the sources of risk that you identify. This would include identifying existing initiatives the company has that could be built upon, as well as GDPR business control gaps that may need to be filled in. Once you have a roadmap, you can assign sponsors to take the lead on those tasks going forward.

Assess, Design, Transform, Operate, and Conform

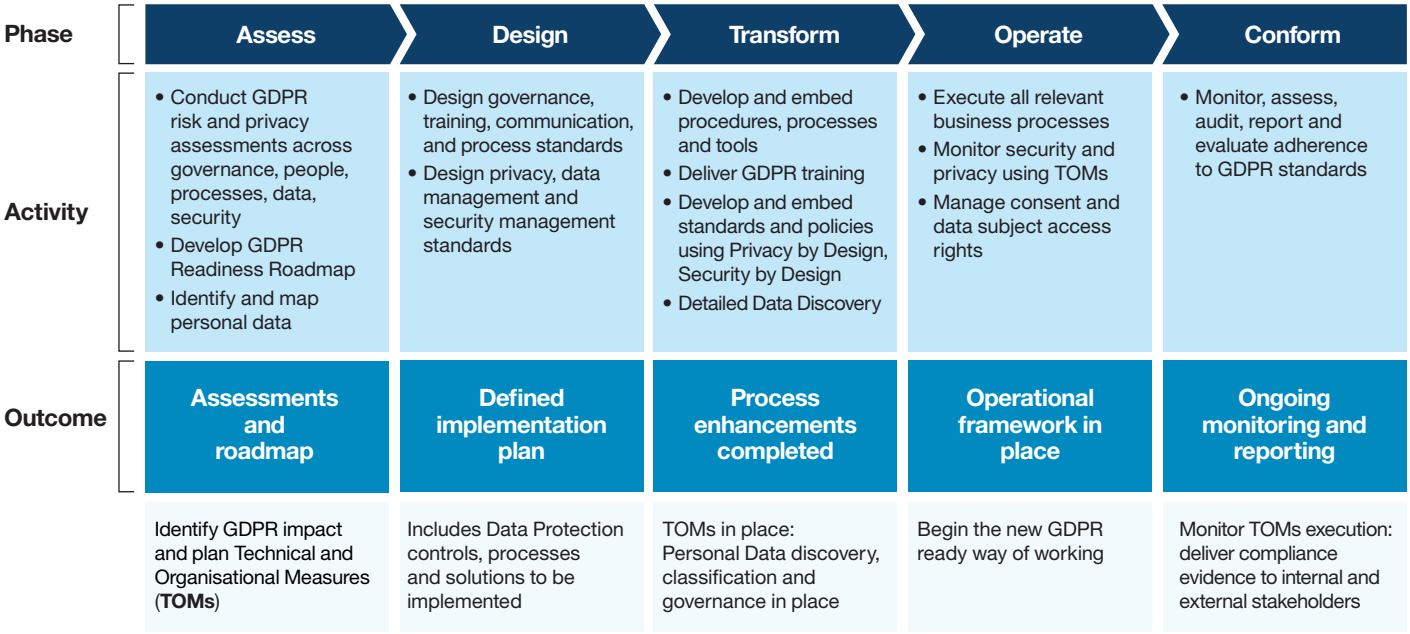


Figure 2: The IBM GDPR framework

IBM has a long-standing proven Data Privacy Consulting Service practice that specialises in these cross-border data privacy compliance challenges and privacy and risk impact assessments. We developed our first Enterprise Privacy Architecture in 2001. This practice has been extended with the acquisition of Promontory Financial Group in 2016. Promontory offers clients a combination of privacy expertise and regulatory risk management experience to guide them through the full lifecycle of building, managing and sustaining GDPR governance programmes. Promontory's team blends experience as former regulators, in-house compliance managers, and global privacy consultants to provide unique perspective and expertise for clients evaluating their GDPR readiness, conducting data-mapping exercises, and developing compliance strategies.

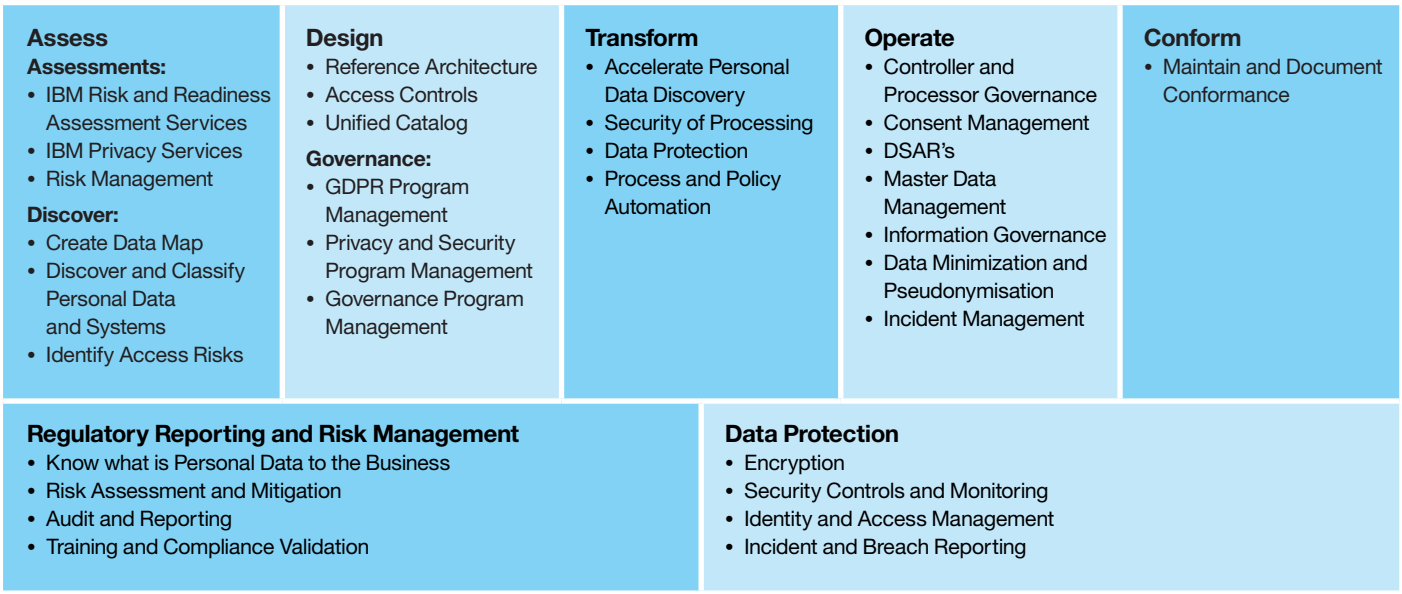


Figure 3: GDPR Framework Pathways

Assess: Risk Management

A regulatory risk management dashboard and dynamic reporting function are both critical programme features for GDPR readiness. They can help to rapidly address any regulatory request or enquiry, with the exception of Data Subject Access Requests (DSARs). IBM's solution for risk and response dashboarding and reporting can help you implement these capabilities. In addition, the IBM Critical Data Protection Program can help you track and mitigate data security risks and classify your organisation's critical GDPR assets, including personal data and other protected information.

Assess: Data Mapping and Personal Data Discovery

When IBM works with a GDPR readiness client, one of the first things we do is find out if the client has a completed data map. If such a data map does not exist, creating one would be a top priority. A data map is key for many reasons, including legal, compliance, security, IT and HR reasons.

It is also very important from a GDPR perspective, because of the DSAR obligations. Your organisation will need to comply with those requests in just one month, and understanding your data characteristics will enable you to meet that deadline. A

data map will also help you discover and document major personal data systems, how data is collected, stored, shared, and transferred, and the nature of the processing. The data map is also a key part of the IBM Critical Data Protection Program, which helps you not only identify and map data assets, but also assess and recommend controls to mitigate risk.

Personal data discovery, which can be completed during or after your GDPR readiness assessment, allows you to deepen your knowledge about how your organisation uses personal data (processes and purposes); what personal data you use (types and sensitivity); and where you hold your personal data (sources). Under Article 30 of the GDPR, this understanding needs to be documented and maintained in a Record of Data Processing Activities. If you don't already have this record, you should create one as soon as possible.

Most organisations have a pretty good handle on where their structured data sources are, but not necessarily what personal data are contained in those databases and transactional data sources. This is the case to an even greater extent for unstructured data sources. Data sources such as old fileshares, shared drives, SharePoint and content repositories are easily forgotten about and thus often contain personal data which is not accounted for properly.

Even in instances when you know you have personal data that needs to be protected, you may not know as much as you should about the volume of that data or exactly which data subjects it applies to. For GDPR readiness, it is very helpful for you to clear out any old data, whilst moving data you do need to keep into the scope of a robust information governance and security programme, so that it can be understood, protected and accounted for in the future.

IBM offers its clients an effective QuickStart GDPR readiness engagement that draws from the power of personal data discovery and catalogue accelerator tools, covering both structured and unstructured data sources. It is designed to generate a clearly defined plan to help you move your GDPR readiness efforts forward within four to six weeks of analysis.

As part of your GDPR readiness engagement, your organisation will be exposed to routines that may be put into place as standardised and repeatable processes to help identify personal data across your data estate. In addition, IBM will work with you to help minimise personal data within your data stores by identifying data you no longer have a valid business reason to keep. Minimising this data—limiting what you store and how long you store it—can help you minimise your GDPR risks and comply with the GDPR data privacy principles such as data minimisation or storage limitation.

You can get started with discovering the personal data your organisation handles in as little as two months from implementation. The additional IBM Accelerators for finding and classifying personal data rapidly expand the diversity, volume and variety of personal data you can discover, even if you haven't formally defined personal data to the business.

Design: Access Controls

Once you've established a complete inventory of personal data, it is time to consider who should have access to what data, a concept known as access controls. The IBM solution delivers a single foundation to help you understand and control user access and risks. It connects compliance auditors, IT staff, and business perspectives for a clear picture of identities and their access, controlling access, and helping to ensure user access audit readiness.

Access controls start with discovery, where dormant accounts and access outliers are identified. Next, organisations can establish an access control baseline, which involves using the solution to review and validate existing data access, cleaning up entitlements, and creating roles and access policies. Once the baseline has been established, ongoing security is enabled through granting data access against a GDPR-risk model validation. Monitoring and enforcement occur through managing the data access lifecycle, and continuously certifying access to identify related risks and violations.

Design: Unified Governance Catalogue

A complete and accurate data inventory or catalogue (Figure 4) can create the foundation for a unified information governance strategy for the GDPR. It helps answer questions about where personal data is located, why it is being collected and stored, and who has access. As such, its benefits are not limited to GDPR readiness: it can help you comply with other rules and regulations that might affect you, now or in the future. It is also the first step toward driving more informed business outcomes by making valuable data available to business users throughout the organisation.

Transform: Data Discovery

Continuing to build on the foundation established during the GDPR readiness assessment, data discovery is where you will consolidate everything you have learned about your personal data, including the sources of that data and their physical location.

At IBM, we believe the best way to create a complete and up-to-date data inventory is to combine a bottom-up approach (using data inventory tools) with a top-down mapping approach (conducting interviews with business and technical users to get a first-hand look at what data resides where, and what business value users draw from that data). This process should be iterated over time, to keep up with changes as they occur.

Figure 4: Unified Governance Catalogue key capabilities

IBM personal data discovery accelerator tools can help you accelerate and enhance the data mapping process for both structured and unstructured data, across on-premises and cloud environments. By quickly analysing and classifying the contents of your data stores, these tools — working in concert with a central unified information governance catalogue and risk response framework — can help you create a detailed catalogue of personal data stores, locations, purposes, owners, data subject types and more.

Transform: Security of Processing

Organisations are required to protect personal data adequately, taking into account the risk to the data subject. To that end, effective security controls are equally applicable as GDPR security controls. The IBM solution provides a "Security Immune System" (Figure 5) that forms a foundation for identifying, correlating and mitigating threats across the various security domains using deep analytics, cognitive computing, and orchestration. Like your body fighting the flu, the security immune system is focused on three things: prevention, detection and response.

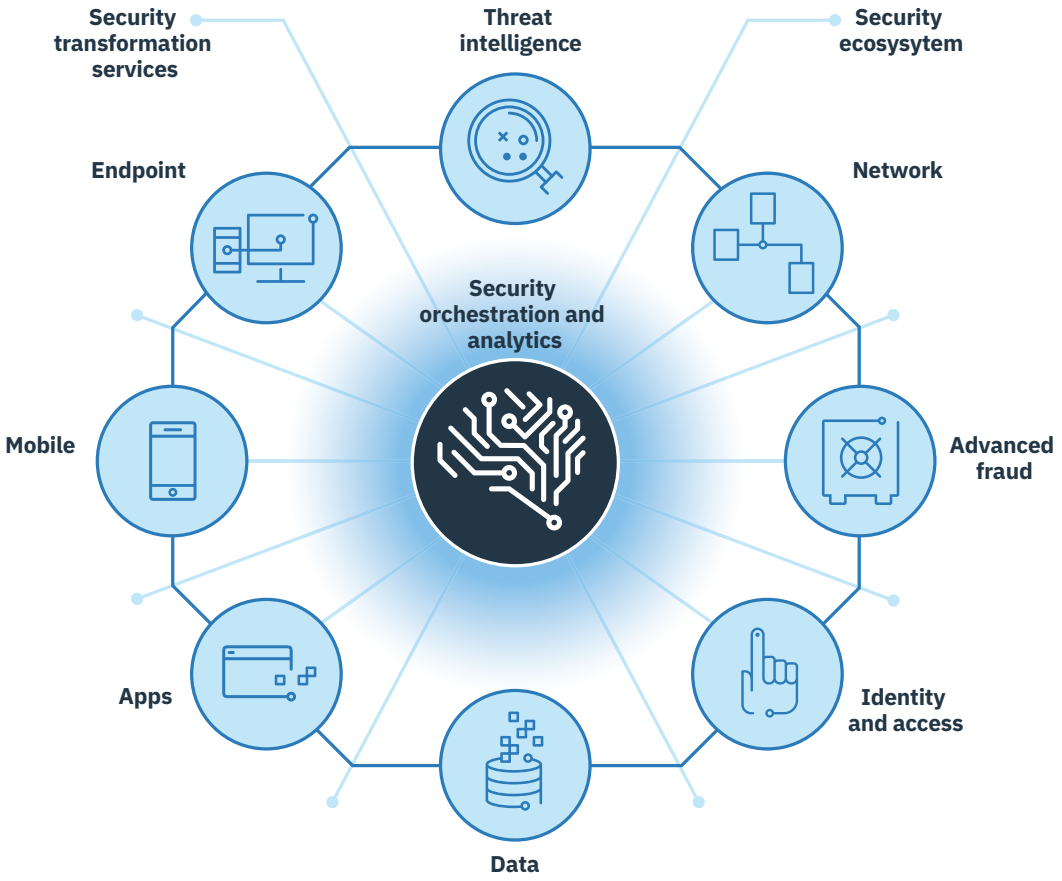


Figure 5: IBM Security Immune System

Further, IBM's 10 Essential Security Practices review can help you understand your current security maturity, and recommend actions you can take to improve it. In particular, the review is designed to help you understand current threats, security strategies and objectives; assess domain effectiveness, document findings and gaps; and establish a roadmap for successful implementation.

Whilst the technology details for security are left to the organisation, the GDPR does mention two specific controls: encryption and pseudonymisation. Pseudonymisation is a technique whereby information cannot be re-identified without additional information. Both masking and encryption are examples of pseudonymisation. Encryption is particularly important since, according to GDPR Article 34, communication of a personal data breach to the data subject may not be required if personal data was rendered unintelligible to any person who is not authorised to access the data. According to the Ponemon 2017 Cost of a Breach study, encryption has been shown to reduce breach costs by over 11 per cent.

Operate: Masking, Encryption and Redaction

IBM solutions can assist you with GDPR readiness by providing capabilities for data encryption. Included are file and database encryption, tokenisation, and application encryption, plus the ability to encrypt and re-key data without taking applications offline. Together, these capabilities help protect data from unauthorised access, minimising the risk that the data might be inadvertently accessed. IBM can also empower your organisation to pursue the principle of data minimisation. Information is de-identified wherever possible, and only the data points that are needed for processing activities such as analytics and testing are preserved.

Using a variety of different masking techniques, IBM can help protect data such as telephone numbers, national identification numbers, email addresses or names in test systems without losing the underlying contextual meaning. Simply put, a masked email address still looks like an email address, and functions like one in test workloads, without putting the address itself at risk of exposure.

Masking can be performed across cloud and on-premises workloads, with predefined data privacy classifications and rules designed to speed time to implementation and simplify your reporting needs. This capability can also potentially reduce the consent duties and obligations.

Operate: Incident Management

The 72-hour breach reporting window is a short one that could greatly benefit from automation. IBM provides tools and services to help you automate, collaborate, and deploy proactive incident readiness, management and reporting capabilities to meet GDPR obligations. Augmenting an incident response platform and incident response services are capabilities for all elements of a breach investigation, including reporting to the relevant supervisory authority.

A GDPR Accelerator is available that includes a GDPR Data Security Impact Assessment, along with predefined sets of policy rules and groups that help monitor, audit, record, and provide alerts on any unauthorised activities related to personal data by privileged and unprivileged users and applications. These same rules are also used to create audit trails for DSARs, such as requests for personal data access, rectification, erasure or transfer.

Reports to identify who accessed personal data, where they accessed it from, when it was accessed, and how it was accessed can be used to send notifications to auditors, controllers and data protection officers using the data security compliance review process in the Accelerator. Also, the Accelerator integrates with IBM's data encryption technologies to facilitate putting additional data protection in place.

Conform: Documenting Conformance

Another aspect of Security of Processing is documenting your conformance. IBM solution capabilities can help in that regard by providing data and file activity monitoring to create audit trails of personal data access with detailed reporting. This data-specific and file-specific access monitoring allows you to see who is accessing which pieces of personal data. By performing real-time and right-time analytics data monitoring, these capabilities can alert security teams in real time if there's suspicious activity occurring around personal data. They can also dynamically block access to that data, quarantine the user ID, or let access proceed whilst alerting the security team.

Additional Pathways to address

Although we believe the Pathways above are the most logical starting points for the majority of organisations preparing for the GDPR, there is a variety of other areas you can also prepare for and address, after you've taken the basic first steps. IBM's solution platform for the GDPR lets you engage some or all of these capabilities to progress your journey toward GDPR conformance.

Operate: Controller/Processor Governance and Vendor Management

Control and management over your processors is one of the fundamental requirements of the GDPR. As a controller, you need to manage your processors and understand their activities around protected data. This can include the need for an effective vendor/supplier management organisation, identification of processors who process personal data subject to the GDPR, development and maintenance of TOMs, and well-defined audit practices. As a processor, you need to participate in audits, handle DSARs, and generally be available for any reasonable controller requests.

Operate: Consent Management

Validating that personal data is used appropriately and the processing has a legal basis, such as consent for the specific purpose, is a key GDPR obligation. Unfortunately, most applications today have an all-or-nothing approach to privacy and consent. The challenge is linking privacy policies to the technical governance and enforcement controls. In response to this, IBM has developed a data privacy and consent management solution to help simplify consent for enterprises and provide more control over how and when data is used.

Data Subject Consent Management is a capability that lets the business inform the end user what data is needed for which purposes. The consent choices made by the end user for each purpose are stored in a central repository for use by all channels—such as web, mobile, and call centres—and all applications in the organisation. There is no need to worry about how to propagate the consent across multiple channels.

Operate: DSARs

The GDPR requires organisations to give data subjects a simple and effective way to exercise their rights of access, correction and erasure. Organisations are required to provide this information without undue delay, and within one month at the latest. This pattern includes case management to track requests, a request portal, identity validation including multifactor authentication, and audit trails to track access and create audit reports. The IBM solution provides frameworks for case management and workflows to expedite DSARs.

Operate: Master Data Management

Master Data Management provides a normalised view of where different sources have pieces of the subjects' personal data, what data you hold for them and precisely where that data is located. This is a critical service capability to support DSAR requests and breach notifications.

Operate: Unified Governance

Unified Governance provides supporting information management processes, which are essentially good housekeeping for data. It can be leveraged along with Content Management to reduce risk and improve economics across all collaborative and unstructured content.

Thinking about the personal data you handle is key to this concept. For unstructured data, organisations should make it their goal to syndicate, instrument and enforce policies regarding mapping, management and security of personal data, both improving information economics and reducing risk. Likewise, for structured data, organisations could implement policy and metadata management, whilst also exploring and managing data lineage, to create information that supports GDPR principles.

Operate: Data Disposal

Removing data that no longer serves a purpose for the business can help maintain data quality and comply with the GDPR principle of storage limitation.

IBM Cloud for GDPR readiness

With IBM Cloud being the first organisation to meet the EU Cloud Data Protection Code of Conduct, you have a one-stop shop for your data privacy, security and information governance needs. IBM Cloud can help your GDPR programme in three ways:

1. IBM Cloud is built for heavily regulated industries and able to meet strict requirements.

With IBM Cloud, you can be assured that we are adhering to our regulatory and compliance commitments to enable GDPR readiness. IBM has signed up more IaaS and PaaS services to the EU Cloud Code of Conduct than any other company: 24 so far. Signing up to the Code, which includes elements of the new GDPR, means we are well placed to help clients implement the trusted infrastructure and services that can form the foundation for an end-to-end compliant enterprise. IBM Cloud holds certifications like ISO 27001, FedRAMP and FISMA and approval from industry-specific standards like HIPAA, PCI, FDA and KBV. In addition, IBM Cloud holds and meets more than 14 certifications and industry standards.

2. IBM Cloud is data first, aiming to give you complete control, visibility and transparency about where your data resides.

Your obligations as controller under the GDPR can be simplified using IBM Cloud. Data residency can help you comply with GDPR data governance requirements. IBM has the largest and most comprehensive European cloud data centre network, with 16 fully operational cloud data centres across Europe. In total, IBM operates 55 cloud data centres in 19 countries across six continents, ensuring that our clients can keep their data local, from a security and regulatory requirements perspective. Giving you complete control and knowledge about where your personal data resides and where it will be processed enables you to reduce data transfer risks.

3. IBM Cloud includes a comprehensive data security platform that can help you meet your GDPR data privacy and security requirements.

IBM Cloud is agile and scalable, with built-in data security and privacy services and solutions that can be consumed on premises or as SaaS offerings. Our comprehensive data security platform helps safeguard sensitive data wherever it resides and provides a full range of data protection capabilities. We are committed to assuring your personal data is secure, encrypted, and protected against breaches. IBM Cloud XaaS solutions align with a range of international and industry standards, such as ISO/IEC 27018, which addresses notification, transparency and documentation requirements of cloud providers for data privacy.

IBM Cloud capabilities to accelerate GDPR readiness:

- Secure virtualisation provides workload security, compliance readiness and encryption capabilities.
- Multi-cloud data encryption helps safeguard data from misuse, whether it resides in a single cloud, multiple clouds or a hybrid environment. This solution encrypts file and volume data whilst maintaining access control, and providing you with control over your keys.
- Key protection enables customers to encrypt personal data at rest and easily create and manage the entire lifecycle of cryptographic keys that are used to encrypt data.
- Cloud-based hardware security modules (HSMs) are standards-based and enable customers to meet regulatory requirements and ensure data security governance.
- Integrated data classification capabilities help create a seamless approach to finding, classifying and protecting your most critical data, whether in the cloud or in the data centre.
- On-demand de-identification throughout the enterprise, including on big data platforms, helps keep confidential data (including personal data) safe.
- The core functions of IBM's global cybersecurity incident management practice are conducted by IBM's Computer Security Incident Response Team (CSIRT). CSIRT is managed by IBM's Chief Information Security Office, and is staffed with global incident managers and forensic analysts. National Institute of Standards and Technology (NIST), the United States Department of Commerce guidelines for computer security incident handling, have informed the development and remain the foundation of IBM's global incident management processes.

Mainframe

For those clients utilising IBM mainframe platforms, native GDPR-ready end-to-end encryption with minimal overhead is also available. This new pervasive encryption capability allows high-performance large-scale data encryption that's highly efficient, transparent, and effective without requiring changes to applications. By encrypting data as it's written, and protecting it both in flight and at rest, IBM mainframe platforms can minimise the need for discovery and classification, whilst making it easier to administer and address compliance.

Understanding your GDPR obligations

As this paper aims to convey, there is nothing simple about GDPR readiness. It's a process that can be complex, challenging and costly, but it is also necessary. In addition to the simple fact that it helps you avoid serious penalties, GDPR readiness can now be considered a cost of doing business when it comes to successfully interacting within the European Union.

In addition, we believe the implementation of the GDPR may be the first step toward opening up a single digital market across Europe. Taking action now can put your organisation in the best position to succeed in that new reality.

Complying with the GDPR is also a great way to gain the confidence of your customers and employees, increase visibility and understanding around your business, make quality data available to every business user, become more efficient, and potentially identify new and better revenue-generating opportunities.

Now that we have shared our perspective towards GDPR readiness, leverage our prescriptive Pathways to help you get started on your journey toward compliance.

For more information

To learn more about the IBM perspective and capabilities for GDPR readiness, visit us today at **ibm.com**/gdpr, or contact your IBM representative.

© Copyright IBM Corporation 2017

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
September 2017

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NONINFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

1 (http://www.efta.int/eea-lex/32016R0679)

2 The Privacy Advisor, "ICO's Wood: GDPR grace period? No way." (https://iapp.org/news/a/icos-wood-gdpr-grace-period-no-way)

3 Article 12 (https://gdpr-info.eu/art-12-gdpr/)

4 Working Party 29 DPO (http://europrivacy.info/2017/04/11/final-dpo-guidelines/)

5 (**ibm.com**/security/data-breach/)

Please Recycle