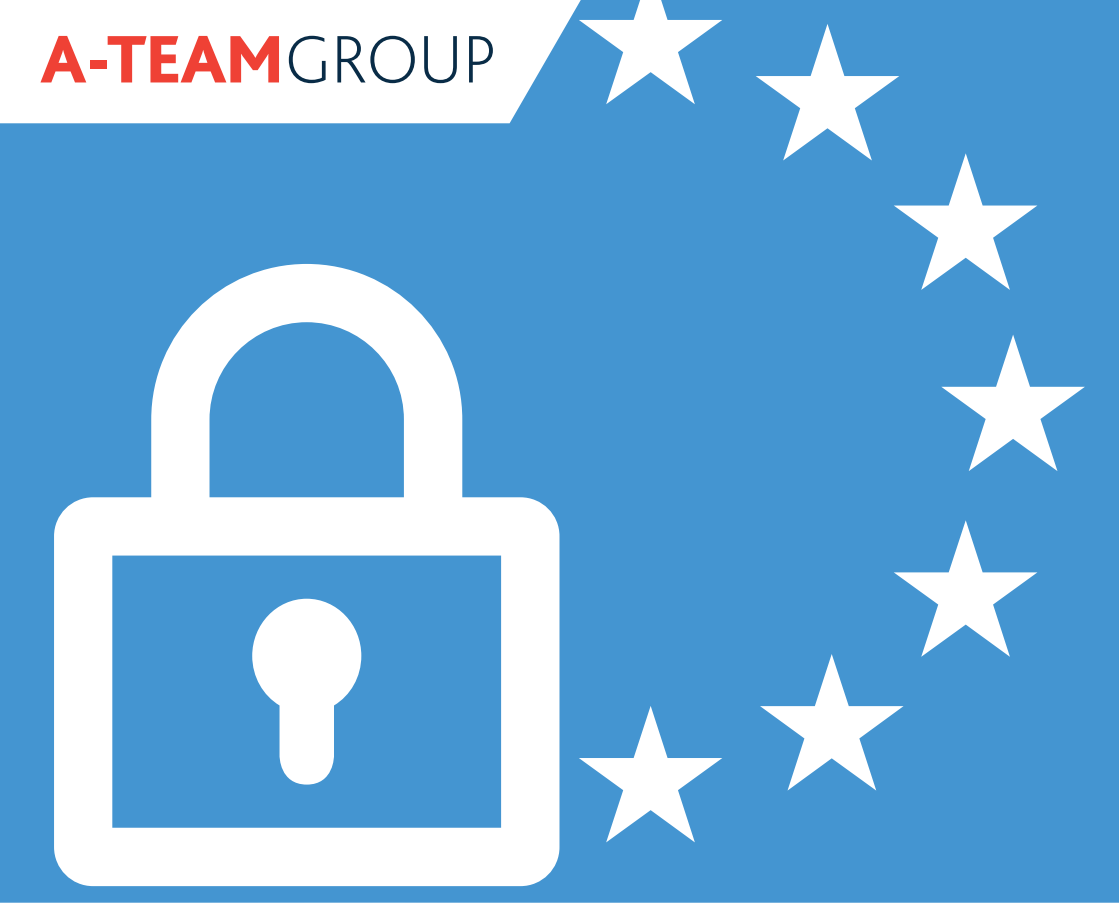
A-TEAMGROUP



GDPR HANDBOOK 2018

Track Personal Information through Every Data Transformation

Build Compliance Confidently with Data Lineage from ASG Technologies

ASG's powerful Enterprise Data Intelligence solutions enable you to effectively manage and govern data within your company.

Data lineage with ASG can track and trace all use of protected personal data. You can create reports to demonstrate protection by design with a data inventory or catalog of protected data that demonstrates your business knows how data are stored within the data estate and how they are used.

Discover more about ASG Technologies GDPR compliance solutions, visit www.asg.com/GDPR.

Contents

A-TEAMGROUP

Editor
Sarah Underwood
sarah.underwood@a-teamgroup.com

A-Team Group
Chief Executive Officer
Angela Wilbraham
angela@a-teamgroup.com

President & Chief Content Officer
Andrew P. Delaney
andrew@a-teamgroup.com

Editorial
Sarah Underwood
sarah.underwood@a-teamgroup.com

Sales
James Blanche
james@a-teamgroup.com
Jo Webb
jo@a-teamgroup.com

Marketing Operations Manager
Leigh Hill
leigh@a-teamgroup.com

Director of Event Operations
Jeri-Anne McKeon
jeri-anne@a-teamgroup.com

Events Content Manager
Lorna Van Zyl
lorna@a-teamgroup.com

Group Marketing Manager
Claire Snelling
claire@a-teamgroup.com

Social Media Manager
Jamie Icenogle
jamie@a-teamgroup.com

Sales & Marketing Operations Support
Jane King
Jane@a-teamgroup.com

Client Services Manager
Ron Wilbraham
ron@a-teamgroup.com

Production Manager
Sharon Wilbraham
sharon@a-teamgroup.com

Design
Victoria Wren
victoria@wr3n.com

Postal Address
Church Farmhouse
Old Salisbury Road
Stapleford, Salisbury
Wiltshire, SP3 4LN
+44-(0)20 8090 2055
info@a-teamgroup.com
www.a-teamgroup.com
www.datamanagementreview.com
www.intelligenttradingtechnology.com

A-TEAMGROUP

Call 020 8090 2055

As a marketing or business manager, you know you need content marketing if you're going to succeed in attracting and engaging with today's more savvy buyer. But do you:

- Struggle to find time to create content consistently?
- Find it hard to think of fresh topics to write about?
- Lack the capacity to generate blogs, run or moderate webinars, seminars or events or other valuable content?
- Fail to generate enough leads or sales conversions from your marketing efforts?

You're not alone. While 93% of marketers use content marketing today, their top two challenges are a lack of time (69%) and producing enough content (55%)*

Come to the content experts at A-Team Group.

A-Team Group has, since 2001, been delivering distinguished content based on in-depth domain expertise on behalf of B2B financial technology suppliers. Run by experienced business journalists, we thrive on taking complex business and technology topics and turning them into compelling content assets to drive lead generation and prospect nurturing with a measurable ROI.

Whether you just need support with content for your blog or to manage a webinar, or if you want the full service content marketing strategy and execution, A-Team Group have the experience, knowledge and content know-how to help you succeed.

* Source: 2013 survey of 1,217 respondents across a range of industries, functional areas and company sizes, by Content Marketing Institute, MarketingProfs and Brightcove.

For a free consultation or to ask any questions, give us a call **020 8090 2055** or email **angela@a-teamgroup.com**

The challenges and opportunities of GDPR

Welcome to our handbook on General Data Protection Regulation (GDPR), a regulation with a significant impact on financial institutions that must review data protection processes, align technology with requirements, respond to data subjects' rights, and sustain ongoing compliance.

Getting GDPR right has several operational and business benefits, including reduced cost, improved data governance, and an accurate view of personal data that can support better customer service and product innovation. Getting it wrong could be disastrous, with fines running up to €20 million or 4% of global annual turnover, whichever is the greater, and reputational damage highly likely as data breaches at organisations processing personal data will be made public. At worst, GDPR could be the downfall of organisations that don't get it right.

With just a few months to go before the GDPR compliance deadline of May 25, 2018, we have scrutinised the regulation, discussed its impact with data management practitioners, and looked at best practice approaches to its many requirements. Based on our investigations, this handbook details data subjects' rights under the regulation, provides a preparation plan, addresses data management problems and outlines feasible solutions.

It also considers the benefits of compliance, notes the fines and penalties of non-compliance, and touches on how GDPR may pan out in months and years to come.

We'll continue to monitor GDPR in the run up to compliance and beyond, and we'll keep you up to date on developments with blogs on our Data Management Review web site – www.DataManagementReview.com – and webinars looking at various aspects of the regulation. You can find out more about these and sign up for our weekly newsletter on the web site.

Meantime, good luck with your implementation of GDPR!

Andrew Delaney
Chief Content Officer
A-Team Group

Foreword

By John Mason, Head of Regulatory & Market Structure Strategic Response & Propositions, Thomson Reuters

General Data Protection Regulation (GDPR) represents a significant change to existing data privacy rules established in the European Union. Its aim is to harmonise data privacy across the region, improve data protection for EU residents, and ensure data security at all times. The compliance deadline is May 25, 2018 and fines for non-compliance are draconian, running up to 4% of group turnover or €20 million, whichever is the greater.

The advances of GDPR on the previous EU Data Protection Directive, which took effect over 20 years ago in 1995, go a long way

The advances of GDPR on the previous EU Data Protection Directive, which took effect over 20 years' ago in 1995, go a long way, giving individuals extensive rights to find out what personal information organisations hold on them and how it is used.

They can also enforce rights to rectify and erase data – essentially the right to be forgotten – restrict processing and move data to between organisations.

All good from an individual's perspective and in line with a widely acknowledged need to improve the security of personal data to guard against misuse, breaches and cyber attacks. For organisations storing and processing personal data, however, the compliance challenge is considerable, requiring personal data to be identified, centralised, maintained and secured, while being open to access. Tools for the task include automation, data lineage, data governance and encryption.

With only a few months to go before the GDPR compliance deadline, many organisations are combining in-house systems already supporting data protection with vendor solutions designed to provide everything from specific elements of compliance to complete renewal of data privacy policies and processes.

The race is on, but the beneficial outcomes for organisations implementing and sustaining successful GDPR programmes go far beyond compliance. As well as gaining a better understanding of the personal data they manage, organisations can improve customer service and product innovation, reduce costs and enhance controls, extend data governance and ensure accountability. But perhaps most importantly, they can build customer confidence, relationships and loyalty.

The race is on, but the beneficial outcomes for organisations implementing and sustaining successful GDPR programmes go far beyond compliance

Overview

General Data Protection Regulation (GDPR) is an EU ruling replacing **Data Protection Directive 95/46/EC** that was established in 1995. The regulation is designed to harmonise data privacy laws across Europe, protect EU citizens' personal information, reshape the way organisations approach data privacy, and ensure personal data processed outside the EU is handled in compliance with the regulation.

Crucially, GDPR focuses on the fundamental rights and freedoms of data subjects, giving them greater control over their data and rights to question organisations about what data they hold, for what purposes, and whether it is shared with other organisations. Other rights of data subjects include data portability and the right to be forgotten.

While GDPR sustains the key principles of data privacy established by the 1995 directive, it extends many of these and clarifies ambiguous territorial applicability set down in the 1995 directive by stating that the regulation applies to all companies processing personal data of data subjects residing in the EU regardless of company location. This means both EU and non-EU based companies processing personal data of data subjects residing in the EU must comply with the regulation. Organisations located outside the EU must also comply if they offer goods or services to EU data subjects.

The regulation extends data protection requirements to include not only controllers, which are in the scope of the

Timeline

January 25, 2012:
European Commission proposes updated data protection regulation

December 15, 2015:
European Parliament and Council of the EU agree final text

April 8, 2016:
GDPR adopted by Council of the EU

April 18, 2016:
GDPR adopted by European Parliament

May 25, 2018:
Compliance deadline

1995 directive and determine the purposes, conditions and means of processing personal data, but also processors that handle personal data on behalf of controllers.

Financial services firms

GDPR does not make distinctions between industries and sectors, but its extensive demands will have a major impact on the financial services sector and require financial firms to reconsider how they build data management systems and manage personal data.

Those that do this well and take a proactive approach to compliance should benefit from improved customer communication, strategic data management and a higher level of trust in the market. For those that breach compliance, the stakes are high – reputational damage and fines up to €20 million of 4% of annual group turnover, whichever is the greater.

The regulation unifies enforcement across the

GDPR principles

Article 5(1) of GDPR requires personal data to be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Controllers and Processors

- Controllers determine the purposes and means of processing personal data. They are required to ensure contracts with processors comply with the regulation.
- Processors are responsible for processing personal data on behalf of controllers. They must comply with legal obligations, such as the requirement to maintain records of personal data and processing activities, and have legal liability if they are responsible for a breach.

Lawfulness of Processing

Article 6 sets out lawful bases for processing. Processing shall be lawful only if and to the extent that at least one of the following applies:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

EU, with each national supervisory authority authorised to take action. Data breaches at financial institutions that are likely to cause significant damage to customers must be reported to the supervisory authority within 72 hours and customers must be notified without undue delay.

Challenges of GDPR

The challenges presented by GDPR include understanding the lawful basis for processing personal data, gaining consent to process the data, building data privacy by design, notifying authorities and individuals of data breaches, ensuring data portability, and giving individuals the right to have data deleted provided there are no legitimate grounds for keeping it.

Financial institutions processing large volumes of sensitive data may need to appoint a data protection officer and will have to carry out privacy impact assessments to identify risks, minimise potential data

breaches and implement data protection strategy.

While financial firms subject to the 1995 directive already have data protection policies and practices in place, it is the detail of GDPR that adds complexity and must be addressed to achieve compliance. For example, general contractual terms will no longer be sufficient to provide proof of consent from individuals to process personal data.

Build your culture of compliance

Thomson Reuters Compliance Learning

Provide your employees with the tools to make the right decisions and protect your business from risk. Thomson Reuters Compliance Learning delivers engaging online training courses that cover a breadth of subjects. Our suite of data privacy courses will ensure you stay on top of the evolving regulations with topics including:

- GDPR in Daily Business
- Regional Data Protection Regulations
- Information Security Awareness

Learn more at risk.tr.com/compliance-learning

The intelligence, technology and human expertise you need to find trusted answers.

the answer company™
THOMSON REUTERS®

Instead, consent must be unambiguous, freely given, informed and refer explicitly to each processing purpose. Consent for processing sensitive data held by banks and financial institutions must also be explicit. The data management requirement here is to consider how customer data is collected, managed and shared with third parties, and develop appropriate consent management policies.

Financial institutions must also respond to the regulation's enhanced rights for individuals to access, transfer and delete data by amending privacy policies and procedures, and the way in which they manage data access requests. The data privacy by design element requires financial institutions to promote privacy and data protection compliance in new system builds.

Security needs to be based on appropriate technical or organisational measures as GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

GDPR has been some years in the making, but was finally approved by the European Parliament on April 18, 2016. It will take effect in all member states on May 25, 2018.

Brexit

The UK will leave the EU in 2019, but this will not change the requirement for UK businesses within the scope of GDPR to remain compliant. The **Information Commissioner's Office (ICO)** has confirmed that if the UK wants to trade with the single market, its data protection standards need to

Preparing for GDPR

Introduction

GDPR is a broad regulation requiring firms to take stock of personal data they hold, understand how it is used, ensure its privacy, and respond to individuals wanting to enforce rights around their data. Some financial services firms are already compliant, many are in the process, and there are, no doubt, latecomers with everything to do before the May 25, 2018 compliance deadline. But wherever a firm is on the journey, getting GDPR right is imperative to avoiding astronomical fines and suffering significant reputational damage.

A plan for preparation

Many of GDPR's principles are similar to those of the Data Protection Directive of 1995, so for firms already complying with the directive this is a good starting point, although there are new elements and enhancements that need to be implemented to ensure transparency and provision of individuals' rights under GDPR.

The regulation also puts greater emphasis on the documentation that data controllers must keep to demonstrate their accountability, calling for an enterprise-wide approach to managing data privacy and improved data governance.

On these bases, a GDPR preparation programme should cover the following issues, many of which are detailed in other sections of the handbook.

Personal data

GDPR defines personal data as any information that can directly or indirectly identify a natural person. It can be in any format. The regulation places stronger controls on the processing of special categories of personal data, which have been extended to include biometric and generic data.

Personal data

- Name
- Address
- Email address
- Photo
- IP address
- Location data
- Online behaviour (cookies)
- Profiling and analytics data

Special categories of personal data

- Race
- Religion
- Political opinions
- Trade union membership
- Sexual orientation
- Health information
- Biometric data
- Genetic data

Awareness: Ensure your organisation understands the impact of GDPR and can identify any issues that could cause compliance problems. Senior management buy-in is essential and large organisations may need to look at resource allocation.

Data: Document all personal data that is held by the organisation, including data that falls into special categories, where the data came from, and any other organisations it is shared with. An information audit across the organisation or within particular businesses may be necessary. GDPR also requires data processing activities to be recorded. For example, if inaccurate personal data is shared with another organisation, the inaccuracy must be communicated to ensure both organisations correct the data. This action must be documented.

Communicating privacy information: Current privacy notices should be reviewed and amended in line with GDPR requirements. Personal data collection currently requires giving people information such as the organisation's identity and how it intends to use the information. Under GDPR there are additional requirements, including

Act now

- Understand how GDPR affects your organisation: Businesses are going to be impacted by the rules in different ways so carry out a full assessment of which changes apply to your organisation and the areas that present the greatest risk
- Escalate to the top of the business: It's crucial that the board understands the enormity of GDPR, the resource needed to transform the way the organisation handles personal data, and the risks of not complying
- Assume full responsibility: The law will hold organisations fully responsible for meeting GDPR data requirements, so make sure your organisation reviews existing systems, procedures and contracts with third-parties to avoid fines
- Appoint a project owner: Depending on the level of change required in your organisation, consider appointing a project owner, a chief data officer or external partner to oversee GDPR readiness
- Welcome GDPR as an opportunity: Personal data is at the heart of a modern organisation's operations and this is an excellent time to make sure the level of protection in place is fit for the digital era. Staying within the law is one thing, meeting changing customer expectations is equally important.

Individuals' rights set out by GDPR

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making including profiling

the need to explain the lawful basis for processing the data, retention periods, and individuals' rights to complain to supervisory authorities if they think there is a problem with the way their data is being handled.

Individuals' rights: Policies and procedures should be checked to ensure they cover individuals' rights under GDPR. The rights are: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and the right not to be subject to automated decision-making including profiling.

In great part, the rights of individuals under GDPR are the same as those under the Data Protection Directive – or the Data Protection Act as the directive is interpreted in UK legislation. The right to data portability is new, but only applies to personal data an individual has provided to a controller where processing is based on an individual's consent or for the performance of a contract, and when processing is carried out by automated means. All personal data must be provided in a structured, commonly used and machine readable format, and must be free of charge.

Subject access requests: Plans should be made to handle access requests taking into account GDPR rules. In most cases, organisations will not be able to charge for complying with a request; organisations will have a month to comply, rather than the current 40 days; organisations can refuse or charge for requests that are manifestly

unfounded or excessive; if a request is refused, the individual must be told why and that he or she has the right to complain to the local supervisory authority and claim a judicial remedy.

Organisations handling a large number of access requests should consider the logistics of having to deal with requests more quickly, and whether systems should be developed to allow individuals to access their information online.

Lawful basis for processing personal data: Organisations need to review and be able to identify their lawful basis for processing personal data, document the lawful basis, and explain it in privacy notices. While a lawful basis for processing does not have many practical implications under current law, GDPR modifies some individuals' rights depending on the lawful basis for processing their personal data. Be aware, for example, that individuals have a stronger right to have data deleted where an organisation uses consent as the lawful basis for processing.

Consent: Firms should review how they seek, record and manage consent and make changes where necessary. GDPR requires consent to be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must be separate from other terms and conditions, and there must be simple ways for individuals to withdraw consent.

There is not necessarily a need to repaper or refresh existing consents for GDPR,

although where there is reliance on individuals' consent to process their data, make sure the consent meets the GDPR requirements above. If it doesn't, alter consent mechanisms and get fresh GDPR compliant consent, or identify an alternative lawful basis for processing individuals' personal data.

Data breaches: Procedures need to be in place to detect, report and investigate personal data breaches. GDPR introduces a duty for all organisations to report certain types of data breach to their supervisory authority, and in some cases, to individuals. A breach only has to be notified where it is likely to result in a risk to the rights and freedoms of individuals.

Data privacy by design and data protection impact assessments: GDPR makes privacy by design a legal requirement and data protection impact assessments (DPIA) mandatory in certain circumstances, particularly when data processing is likely to result in high risk to individuals. Organisations should assess where DPIAs may be necessary, who will run them, and whether they should be run centrally or locally.

Data protection officer: Organisations must consider whether they need to formally designate a data protection officer (DPO) on the grounds that they are a public authority or an organisation that carries out regular and systematic monitoring of individuals on a large scale. If an organisation needs a DPO, someone must be designated to

take responsibility for data protection compliance and a decision must be made on where the role will sit in the organisation's structure.

Cross-border processing: Organisations carrying out cross-border processing within the EU must determine a lead data protection supervisory authority and document this. The lead authority is the supervisory authority in the state where an organisation's central administration is located or the location where decisions about the purposes and means of processing personal data are taken and implemented.

Data management

Introduction

As well as gaining a business understanding of GDPR, firms need to focus on the data and data management challenges it presents, including identifying personal data, managing it within the scope of the requirements, and ensuring it is secure and accessible. Data management solutions include data centralisation, master data management, data governance and automation, all of which must be sustained and continually updated as GDPR compliance is an ongoing, rather than one-off, exercise.

The regulation includes 99 articles, of which 64 are general and cover areas such as objectives, scope, definitions, requirements, liabilities and penalties. The remaining 35 articles are actionable and include 15 related to business, and requiring actions such as setting policies, 7 covering assessment of areas such as infrastructure and deployment, and 13 including technical detail about what data controllers and processors must do to achieve compliance.

Among these technical articles, Article 30 is often cited as one of the more difficult to implement as it requires controllers and, to a more limited extent, processors to maintain records of processing activities. The records must cover information such as the name and contact details of the controller; a description of categories of data subjects and personal data; categories of recipients to whom the personal data has been or will be disclosed; transfers of personal data to a third country or an international organisation; and the purposes of the data processing, which are often problematic to identify, particularly in the early phases of a GDPR programme.

As well as these challenges, data management for GDPR compliance generates some unintended consequences that must be considered.

Identifying personal data

GDPR requires personal data to be processed in a way that ensures its security. This includes protection against unauthorised or unlawful processing and accidental loss, destruction or damage, and requires appropriate technical and organisational measures to be put in place.

With such a wide remit, every GDPR programme needs to start with senior management buy-in, participation of stakeholders across the organisation, and a commitment to adhere to data privacy policies and processes. By building data privacy into the organisation, it becomes possible to achieve immediate compliance, ongoing alignment with the regulation, and avoidance of potentially large fines for non-compliance.

With buy-in from the business, personal data can then be identified and located across the organisation. It could be stored in traditional systems, such as customer relationship management and sales systems, or it could be hidden in unstructured data sources such as emails. This is where data filtering, sampling techniques and algorithms come into play, allowing organisations to identify and extract personal data from both structured and unstructured data sources.

Understanding different applications and contexts of personal data is also important as most organisations know their customers and employees in a number of different ways, making it necessary to map and match disparate data to get a single profile of personal data. An example here is an airline, which may know a

customer through a Twitter account, as a passenger, and as a frequent flyer, and must pull this information together to have a complete picture of the customer's personal data.

A top-down approach to identifying and managing personal data asks business owners to identify data they use, where it is located, and how it is used. The GDPR team can work with the business owners to get a clear understanding of business processes involving personal data and consider aspects such as whether consent has been obtained for a particular process, who is the controller, what type of data is being collected, how long it must be retained, and who is responsible for the data.

Once processes have been analysed in this way, they can be catalogued and maintained within a data governance platform.

At its simplest, a bottom-up approach brings in employees to support data discovery and communicate data protection issues on an ongoing basis to data stewards or the GDPR team leading the compliance programme.

On a more technical level, a bottom-up approach could

use metadata management tools to identify personal data, categorise the data and assign GDPR attributes to it. The metadata can be loaded into a data governance platform and used to identify data elements relevant to GDPR. Once data processes and data elements are identified and governed, they can be linked and data elements used in particular processes can be mapped.

Another early consideration, particularly for organisations working across multiple jurisdictions, is to define personal data that carries different labels – perhaps a social security number in one jurisdiction and a tax code in another – and ensure all instances of the data are identified.

Unauthorised applications and services implemented by end users must also be discovered and personal data identified. Data scanning may well miss these so-called rogue systems, but their content is as much within the scope of regulation as the content of an organisation's mainstream systems.

In situations where data is held either physically or electronically by third-parties with no access to, or knowledge of, the content, responsibility for the data must be assigned. In most cases, responsibility lies with the sponsor of the information, although it is wise to put documentation in place to confirm or qualify this.

A top-down approach to identifying and managing personal data asks business owners to identify data they use, where it is located, and how it is used

Data capture and centralisation

To achieve best practice GDPR compliance and prove where personal data is, and isn't, organisations need to capture the data, make a data inventory and create a central data repository. This will ease the challenge of identifying and sustaining personal data workflows

Challenges of data centralisation

- Legacy systems
- Data silos
- Derived data
- Big Data
- Spreadsheets
- Collaboration tools

by ensuring disparate data is reconciled, data is maintained, entitlement policies are in place, and access to personal data is available to data subjects.

The capture of personal data must bring with it necessary consents to process the data for particular purposes. Existing data protection policies may meet the levels of consent required by GDPR, but most organisations will need to review and renew consents with data subjects using either a personal 'go to' or automated, online 'self service' approach.

Centralisation presents an opportunity to remediate personal data and remove any that is no longer needed, reducing the risk of breaching GDPR requirements

The challenges of data capture and centralisation include legacy systems, which may need to be replaced if they hold customer data but do not have the security or accountability required for compliance, data silos, derived data, multiple tables in Big Data environments, spreadsheets and the use of SharePoint document management and storage, all of which scatter personal data, often multiple times, across an organisation with no clear view of which version of information, if any, is correct, up-to-date, maintained and carries consent.

Solutions to the problem include technology tools and techniques that support the identification and capture of personal data wherever it is. For most firms, and particularly those with hundreds or even thousands of servers, the need is to minimise the number of locations holding personal data and use automated tools to analyse and consolidate the data.

Master data management (MDM) is also helpful in marshalling data and reconciling it to create a data warehouse containing master data records of personal data. In the context of GDPR, this

data can then be used across services and applications that individuals opt into.

The centralisation of personal data has obvious advantages, such as the provision of a 'single version of the truth', greater control and relatively easy access. It also presents an opportunity to remediate personal data and remove any that is no longer needed, in turn reducing the risk of falling foul of GDPR requirements.

A risk-based approach

GDPR presents a risk-based framework that encourages controllers to engage in risk analysis and provide risk-measured responses. Therefore, most organisations are taking a risk-based approach as the best way to achieve compliance, or at least, a sufficient level of preparation towards compliance to show intent and avoid regulatory penalties.

This approach looks first at implementing policies and procedures that will protect high-risk areas where data of an explicitly personal nature is held and if breached could expose a data subject to significant risks, perhaps a personal email address or phone number.

Information of a sensitive nature, such as passport identification provided for Know Your Customer (KYC) or Anti-Money Laundering (AML) purposes, should also be viewed as high risk.

Lower-risk areas, often business-to-business in nature and including data such as the business email address of a customer, must be protected, but if necessary can be addressed with less urgency.

Throughout the regulation, organisations that control the processing of personal data are encouraged to implement protective measures corresponding to the level of risk of their data processing activities. The regulation doesn't define how organisations should assess and quantify risk, although its obligations provide guidance on levels of protection.

For example, the regulation sets out heightened requirements for controllers that engage in high-risk activities in Articles 32, 33 and 34. Specifically, before engaging in high-risk activity, an organisation may be required to consult with a supervisory authority and conduct a detailed privacy impact assessment. In the case of a data breach, the organisation may be required to notify potentially affected individuals.

Where activities carry risk, but not high risk, controllers must still adopt measures that are appropriate to the risk level of the activity. For example, controllers are required to 'ensure a level of data security appropriate to the risk' and implement risk-based measures to comply with the regulation's general obligations.

Low-risk activities in which the risk to data subjects is minimal may exempt controllers from the requirement to notify authorities of a data breach. A foreign controller may be relieved of the requirement to appoint a representative in the EU.

Data governance

A data governance programme is critical to complying with the complexities of GDPR and essential to meeting the challenges of identifying, monitoring, accessing and protecting personal data that is stored and processed across a broad range of applications and systems.

Central to GDPR is a requirement that organisations can prove compliance throughout processes that fall within the scope of the regulation. This requires extensive data lineage to be put in place, and data governance policies to be established, documented and enforced across an organisation.

Data governance policies could cover parameters around data subjects' opt-in periods, data retention frameworks and archiving of historical data. They also form

the basis of data processes that meet GDPR compliance requirements. For example, considering the need under GDPR to be able to share data and make it portable, whatever system is used to fulfil data subject access requests must be able to pull together all information held on the individual and transform it into commonly used, shareable formats, so that it is easy to read, understand and transfer should a data subject want to transfer his or her data to another organisation.

Similarly, data governance policies and processes support the audit component of GDPR, which requires organisations to know where data is and how it is being handled. It can also help organisations see who has accessed personal data and how it is protected.

People are also important to data governance, with data stewards taking policies and procedures to users and data owners taking responsibility for business data relevant to their roles.

Many firms already have data governance and lineage in place, and this can be extended to support the requirements of GDPR using either in-house technology and expertise, or vendor solutions. Some, however, will need to start from scratch, or may decide to refresh their solutions.

A data governance programme is critical to complying with the complexities of GDPR and essential to meeting the challenges of identifying and protecting personal data

Typically, vendor solutions are based on platforms that automate data governance and management, and provide trusted data to business users including help desk advisors responding to requests from data subjects about what personal data the organisation holds about them and how it is used.

The data governance element is often an integral element of an overarching GDPR solution including core capabilities

Categories of security

- Assessment
- Prevention
- Monitoring

such as a centralised inventory of personal data, data lineage to track and trace all application use of protected personal data, workflows around personal data ownership, data sharing agreements that dictate how personal data should be shared both internally and externally.

These types of solutions also cover reporting for both business users of personal data and to demonstrate compliance by providing a data inventory or catalogue of protected data showing where the data is stored and how it is used. Alerts for possible non-compliance are also available.

Data security

GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Data security can be split into three categories: assessment, prevention, and monitoring.

To assess security risks, GDPR mandates that controllers carry out data protection impact assessments (DPIAs) when certain types of processing of personal data are likely to present a high risk to the data subject. The assessment must include a systematic and extensive evaluation of an organisation's processes and how they safeguard the data.

At various places in the regulation, GDPR reiterates the importance of preventing security breaches and recommends techniques to prevent an attack from succeeding. These include encryption, which makes data unintelligible to anyone who is not authorised to access it; anonymisation, which scrambles the data and makes it obfusc; and pseudonymisation, which makes it difficult to link a data set to the original identity of a data subject. As well as reducing risks for data subjects, these techniques can help controllers and processors meet their obligations.

Constant monitoring of activities on personal data is critical to detecting anomalies. In addition to monitoring, GDPR requires timely notifications in case of a breach.

To ease the ongoing burden of data security and increase the quality of data protection, GDPR requires data security by design and default, recommends centralising administration when dealing with multiple applications and systems so that breaches can be detected quickly and action taken, and mandates protection of personal data throughout the data lifecycle, including data at rest and in transit, in an effort to counter security threats.

Accountability and governance

In addition to data governance, GDPR provisions promote accountability and business governance complementing the regulation's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, GDPR elevates their significance.

At various places in the regulation, GDPR reiterates the importance of preventing security breaches and recommends techniques to prevent an attack from succeeding

Governance measures must be proportionate and should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

The accountability principle is set out in Article 5 and requires organisations to demonstrate that they comply with the principles of the regulation. It states explicitly that this is the responsibility of the organisation and that organisations need to implement appropriate

technical and organisational measures to ensure and demonstrate compliance.

Technical measures could include data minimisation, encryption, anonymisation, pseudonymisation, transparency, allowing individuals to monitor processing, creating and improving security features on an ongoing basis, and using data protection impact assessments where necessary.

Organisational measures could include internal data protection plans such as staff training, internal audits of processing activities, and reviews of internal HR policies.

Accountability and governance requirements

- Demonstrate compliance with GDPR
- Establish a governance structure with roles and responsibilities
- Keep a detailed record of all data processing operations
- Document data protection policies and procedures
- Carry out data protection impact assessments (DPIAs)
- Implement appropriate measures to secure personal data
- Train staff and raise awareness
- Appoint a data protection officer

Technology

GDPR is an enterprise-wide regulation requiring some firms and leading others to review existing systems and processes, and consider emerging technologies that could improve the accuracy and efficiency of compliance, reduce costs, improve data quality and deliver better customer service. Some of these technologies, particularly automation, are immediately useful, while others, such as machine learning, Big Data and blockchain, need careful consideration in terms of their ability to respond to GDPR requirements for transparency and their limitations in meeting data subjects' rights to understand how decisions have been made using their personal data, request portability, and execute the right to be forgotten.

Automation: The extent of GDPR, pressure on budgets, the quest for data quality and the large volumes of personal data processed by many organisations call

asg technologies®

5 Steps to GDPR Compliance

Pave the way for regulatory compliance with ASG Technologies solutions.

1. Build an inventory of personal data.
2. Establish compliant business processes and policies.
3. Build data lineage across business units and system silos.
4. Leverage automated dashboards and reports.
5. Establish data management best practices for compliance.

Discover more about ASG Technologies GDPR compliance solutions, visit www.asg.com/GDPR.

for automation to achieve speed, accuracy and timeliness, reduce costs and inaccuracies, and replace manual intervention required to get personal data right with a manageable level of exceptions handling. Automation is well suited to support the collection, centralisation and data governance of personal data, and is typically a component of vendor solutions for GDPR compliance.

There are proponents and opponents of using blockchain to support GDPR compliance, but on the whole the technology does not lend itself well to the task

Machine learning: Machine learning is gaining traction in many functions of financial services firms, but its lack of transparency can be a barrier to use in data protection compliance. The problem is that algorithms used in machine learning lack accountability and do not satisfy the regulatory requirement to provide information on how decisions using personal data are made.

At the moment, consensus suggests the use of machine learning and more advanced artificial intelligence (AI) technologies are not well suited to GDPR compliance, although solutions are being investigated, including algorithmic auditing that would bake auditability into algorithms and allow third parties to monitor, review and critique their behaviour.

Big Data: Big Data and analytics raise similar transparency issues and implications for data protection as machine learning. It can be difficult to apply the regulation's principles to Big Data environments as problems arise not only from the volume of data, but also from the ways in which it is generated, propensity to find new uses for it, complexity of the processing, and the possibility of unexpected consequences for data subjects. Again, Big Data and analytics need further development and

transparency if they are to play well into GDPR compliance.

Blockchain: There are proponents and opponents of using blockchain to support GDPR compliance, but on the whole the technology does not lend itself well to the task, in great part because of the regulation's inclusion of data subjects' rights to request data portability and the right to be forgotten.

While blockchain technology and its immutable nature can strengthen data ownership, transparency and trust between entities, thereby improving transaction-based processing, the rights of GDPR mentioned above run contrary to its design, making it very difficult, if not impossible, to store and manage personal data on a blockchain.

Unintended consequences

Like most regulations, data management for GDPR compliance has unintended consequences that are not necessarily beneficial. One of these revolves around individuals' interests in accessing their data. While many individuals will request access because they are curious to know what information companies hold about them, some may make requests if there is a chance of compensation, which is possible if controllers are proved not to be compliant or if personal data is breached. Still more, some individuals may request data access purely to raise a cost against the business and punish it for a negative experience or for a perceived politically incorrect approach to the market.

Another unintended consequence could be restricted access for EU residents and companies to applications of technology. For example, internet start-ups are often based on business models that collect masses of personal information and use Big Data to extract value from it. These start-ups will fall within the scope of GDPR if they store and process personal data of EU residents, but they may struggle to

afford the costs of compliance. In these situations, start-ups may choose not to market their services in the EU, restricting residents' and companies' access to technology applications.

Perhaps not unforeseen, but certainly unfortunate, is that while there is a single GDPR regulation, its multi-jurisdictional scope means there are many iterations of it

A potentially extreme and unintended consequence of the regulation arises from the potentially astronomic fines organisations will face if they experience a personal data breach. The regulation provides little guidance on what exactly must be reported to customers and how in the event of a breach, leaving businesses open to extortion and paying off criminals that have breached their systems rather than facing huge fines and reputational damage.

Perhaps not unforeseen, but certainly unfortunate, is that while there is a single GDPR regulation, its multi-jurisdictional scope means there are many iterations of it, at least one per EU country. This inevitably raises the risk of conflict across versions and jurisdictions.

Aside from these potential conflicts, GDPR raises questions about compliance with other regulations, particularly KYC, AML and other financial crime measures that take a slightly different view of data privacy.

Beneficial outcomes

A successful implementation of GDPR and ongoing management of personal data in line with the regulation can deliver far more than compliance, with financial services firms able to mitigate the risk of draconian fines and reputational damage for non-compliance, as well as gain significant operational and business benefits.

From an operational perspective, the need to create a centralised hub of

personal data can act as a catalyst for data remediation and removal of data that is no longer relevant. It also reduces the risk and expense of storing personal data in many locations, and cuts the cost of internal and external audits. Time to build applications is reduced, again reducing costs and providing competitive advantage.

Beyond cost, compliance ensures security is in place for technologies that house privacy information and reduces liability, while data centralisation allows operations to deliver 'a single version of the truth', along with greater control of, and access to, personal data.

From a business standpoint, the benefits of compliance are many. Governance and accountability improve, data governance takes a major step forward, and firms will have an accurate view of personal data that can support improved customer service, product innovation and responses to data subject requests. They will also have a clear understanding of high risk data processing that will support informed decisions on whether to process data of an explicitly personal or sensitive nature.

The need to centralise and reconcile data provides a trusted source of information, making data science and predictive analytics more viable, and the very fact of compliance builds customer trust, brand image and reputation. So, not only are we talking about benefits within GDPR, but also benefits extending well outside the regulation and helping organisations become more successful.

Individual rights and the data management response

Introduction

The rights of individuals set out in GDPR are extensive and expand on those of the 1995 EU Data Protection Directive. From a data management perspective, responding to these rights can be a challenge, but with personal data in a centralised hub, readily available access to the data, and ongoing data maintenance in place, organisations should be able to rise to the challenge.

Considering the requirements of each right, below is a brief outline of feasible data management responses.

Right to be informed: The right to be informed requires organisations to provide individuals with a large range of information from the personal data they hold about the individuals and the purpose of processing the data, to the existence of automated decision-making processes and how to make a complaint to a supervisory authority.

The data management response requires an individual's personal data to be identified, reconciled, stored centrally in a data repository, linked to information about how it is processed, and be made accessible to the individual either physically or electronically. The information supplied to the individual about the processing of personal data must be concise, transparent, intelligible and easily accessible, written in clear and plain language, and free of charge.

Right of access: Under GDPR, individuals have the right to obtain confirmation that their data is being processed and access their personal data and other supplementary information. The regulation clarifies that the reason for allowing individuals to access

their personal data is to make them aware of, and be able to verify, the lawfulness of the processing.

Again, personal data needs to be centralised to provide a single view of an individual and make his or her data accessible in a secure manner. Information must be provided without delay and at the latest within one month of a request. The identity of the individual making the request must be ascertained using 'reasonable means' and if the request is made electronically, the information should be provided in a commonly used electronic format.

GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system that can provide the individual with direct access to his or her information. Access to data must be free of cost unless requests are manifestly unfounded or excessive, in which case a reasonable administration fee can be charged.

Right to rectification: GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

Data management processes must support the correction or completion of personal data in the central repository for use by downstream systems. If the data has been disclosed to others, processes must be in place to notify each recipient of the rectification. This requires not only internal data management processes, but also connectivity with external organisations with which data is shared. A request for rectification must be answered within one month.

Right to erasure: The right to erasure, also known as the

right to be forgotten, enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have a right to have personal data erased and to prevent processing in specific circumstances, such as where the personal data is no longer necessary in relation to the purpose for which it was originally collected and processed, when the individual withdraws consent, and when the data was unlawfully processed.

There are specific circumstances in which an organisation can refuse to comply with a request for erasure. These include requests where personal data is processed to exercise the right of freedom of expression, to comply with a legal obligation for the performance of a public interest task, for public health purposes in the public interest, for archiving purposes in the public interest, or the exercise or defence of legal claims.

The data management response must support access to, and the removal of, data to be erased from a central data hub, and ensure it is no longer available to downstream applications and businesses that previously used it. If the data has been disclosed to others, processes must be put in place to contact each recipient and inform them of the erasure.

GDPR reinforces the right to erasure by clarifying that organisations in the online environment that make personal data public should inform other organisations that process the personal data to erase links to, copies of, or replication of the data. This can be challenging where personal information is processed online, for example on social networks, forums or websites, but organisations must endeavour to comply with the requirement.

Right to restrict processing: Individuals have a right to block or suppress processing of personal data in certain

circumstances. For example, when an individual contests the accuracy of personal data, processing should be restricted until the accuracy of the data is verified. When processing is unlawful, an individual can oppose erasure and instead request restrictions on processing.

When processing is restricted, organisations can store the personal data, but not process it, and they can retain just enough information about the individual to ensure that the restriction is respected in future.

From a data management perspective, this requires the ability to identify personal data requested for restriction, consider whether it can or cannot be restricted, and execute on the decision. If personal data has been disclosed to others, the recipients must be informed of the restriction on the processing of the data. Individuals must be informed when an organisation decides to lift a restriction on processing.

Right to data portability:
An addition to GDPR, the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. They must be able to move, copy or transfer the data from one IT environment to another in a safe and secure way, without hindrance to usability. The right only applies to personal data an individual has provided to a controller, where the processing is based on the individual's consent or for the performance of a contract, and when processing is carried out by automated means.

The data management requirement here is to provide the personal data in a structured, commonly used and machine-readable format. Suggested open formats include CSV files. Machine readable means the information is structured so software can extract specific elements of the data, allowing other organisations to use it. It is not necessary for organisations to adopt or maintain processing systems that are technically

compatible with those of other organisations. The information must be provided free of charge and within one month of the request to move the data.

Right to object: Individuals have the right to object to processing based on legitimate interests. These include profiling, direct marketing including profiling, and processing for purposes of scientific or historical research and statistics. Individuals' objections must be made on grounds relating to her or his particular situation.

To comply with the right to object where personal data is processed for the performance of a legal task or in an organisation's legitimate interests, data management needs to identify the personal data and stop processing it unless the organisation can demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the individual, or the processing is for the establishment, exercise or defence of legal claims. This type of objection is likely to require exception management.

Processing data for direct marketing purposes must be stopped as soon as an objection is received. There are no exceptions to this.

Individuals must have grounds relating to their particular situation in order to exercise the right to object to processing for research purposes. Where research is conducted and requires the processing of personal data for the performance of a public interest task, there is no requirement to comply with an objection.

Where processing activities that can be objected to are carried

out online, an organisation must offer a way for individuals to object online.

Rights related to automated decision making including profiling: GDPR provides provisions covering automated individual decision-making – i.e. making a decision solely by automated means without any human involvement, perhaps an online decision to award a loan; and profiling – i.e. automated processing of personal data to evaluate certain things about an individual, perhaps to find out about the individual's preferences. The right restricts controllers and processors from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. GDPR Article 4 specifically defines and regulates profiling for the first time.

The data management response to automated decision making and profiling requires organisations to audit systems and processes to ensure they are not operating outside the restrictions, which are only lifted in circumstances where a solely automated decision is necessary for entering into, or performance of, a contract between an organisation and an individual, authorised by law, or based on an individual's explicit consent.

Because this type of processing is considered to be high risk, GDPR requires organisations to carry out a data protection impact assessment (DPIA) to show that risks have been identified and assessed, and how they will be addressed.

Data management processes need to provide transparency to meet the requirement for meaningful information about the logic involved in decision making, as well as the significance and envisaged consequences for the individual. They must also use appropriate mathematical or statistical procedures, support the correction of inaccuracies and minimise the risk of errors. Personal data must be secured in a way that is proportionate to the risk to the interests and rights of the individual.

Data protection officer

Introduction

GDPR requires organisations to appoint a data protection officer (DPO) in certain circumstances, although in effect, the requirement will cover most financial services firms acting as data controllers or processors.

The regulation mandates in Article 37 that a DPO must be appointed if an organisation is a public authority, carries out large scale systematic monitoring of individuals, or carries out large scale processing of special categories of data or data relating to criminal convictions and offences. Exceptions to the mandate include private organisations that monitor data subjects infrequently with little infringement on their rights, or do not process special category personal information at all or only for a small group of data subjects.

That said, the guidelines of the GDPR Article 29 Working Party on Data Protection note that where GDPR does not specifically require the appointment of a DPO, organisations may find it useful to designate a DPO on a voluntary basis. Where this is the case, the requirements under Articles 37 to 39 – covering designation of a DPO, the position of the DPO within the organisation, and tasks of the DPO – apply as if the designation was mandatory.

The working party further recommends that unless it is obvious that an organisation does not need to designate a DPO, controllers and processors should document the internal analysis carried out to determine whether or not a DPO should be appointed, in order to demonstrate that relevant factors have been taken into account. The analysis is part of the documentation under the accountability principle and may be required by the supervisory authority. It should be updated when necessary, for example if controllers or processors undertake new activities or provide new services that might lead to the need for a DPO as specified in Article 37.

The regulation allows a single DPO to act for a group of companies. This could require companies in the group to deploy data stewards or privacy champions with responsibility for data protection in their areas and a dotted line in to the DPO.

It also provides for an existing employee to be allocated to the role as long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. The role can also be contracted out. Information about the DPO must be published publicly and provided to regulatory oversight agencies.

DPOs are not personally responsible in cases of non-compliance with the GDPR. The regulation makes it clear that compliance is a responsibility of controllers or processors.

While a DPO, where mandated, must be in place before the GDPR compliance deadline in May, the challenge for many companies is to identify suitable internal candidates or hire externally from a pool that is likely to dry up as the deadline approaches.

The role of the DPO

The role of the DPO is high profile and carries significant responsibility and accountability. The minimum tasks of a DPO are defined in Article 39 of the regulation and can be summed up as:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with GDPR and other data protection laws, including managing internal data

protection activities, advise on data protection impact assessments, and train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed
- To have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

The employer of the DPO must ensure that:
- The DPO reports to the highest management level of the organisation – i.e. board level
- The DPO operates independently and is not dismissed or penalised for performing their task
- Adequate resources are provided to enable DPOs to meet their GDPR obligations

The skill set

GDPR does not specify the precise credentials a DPO is expected to have, but does require the DPO to have professional experience and knowledge of national and European data protection law, and a deep understanding of GDPR. The DPO's experience should be proportionate to the type of processing an organisation carries out, taking into account the level of protection the personal data requires.

Considering the tasks of the DPO above, the role is likely to be at senior executive level and include significant management, communication, education and collaboration capabilities, as well as the ability to build strong relationships internally between business and IT, and deal externally with data subjects and supervisory authorities.

GDPR want to learn more?

We have a wealth of information available to help you prepare for GDPR today

White Paper

bit.ly/GDPRChallenges

How to Tackle the Challenges of GDPR

Webinars: Upcoming & Recordings

bit.ly/DMR-Webinars bit.ly/DMR-Webinars-OnDemand

Best practice data governance for GDPR compliance: March 15

Countdown to GDPR: April 24

GDPR Programme Insights for GDPR Readiness: On Demand

Events

bit.ly/ATeam-Events

March 22: Data Management Summit - LONDON

September 20: Data Management Summit - NYC

October 4: RegTech Summit for Capital Markets - LONDON

November 15: RegTech Summit for Capital Markets - NYC

A-TEAMGROUP

Data protection by design and default

Introduction

Data protection by design and default – often known as privacy by design and default – is an approach that promotes privacy and data protection compliance from the start of a project, through its lifecycle and on to its closure. It can apply, for example, to building new IT systems for storing or accessing personal data, data sharing initiatives, or using data for new purposes. It also includes privacy impact assessments (PIAs).

GDPR does not explicitly require organisations to retrofit privacy by design into existing systems, although in the UK this is encouraged by the Information Commissioner's Office (ICO).

Data protection by design and default is not a new concept and was originally introduced by the Canadian Privacy Commissioner of Ontario back in the 1990s. It has since been adopted by regulators from around the world as a component of data protection.

GDPR privacy by design and default set down in Article 25 of the regulation is a formal recognition of the requirements of the 1995 EU Data Protection Directive. The directive includes no specific requirements for data controllers to implement privacy by design and default, and instead requires data

Article 25

"Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

controllers to implement technical and organisational measures to protect data against unlawful processing. The inclusion of data protection by design and default in the principles of GDPR acknowledges that privacy cannot be ensured by legislation and that it needs to be considered in the design and maintenance of information systems.

Article 25

Article 25 of GDPR covers both privacy by design and privacy by default. Moving beyond the 1995 directive, the first paragraph of the article, which covers privacy by design, requires controllers to implement appropriate technical and organisational measures both at the time of determination of the means for processing and at the

time of the processing itself. This ensures compliance with principles such as data minimisation. Privacy by design measures could include pseudonymisation or other privacy enhancing technologies.

Conducting a privacy impact assessment involves working with people within the organisation, with partner organisations and with data subjects to identify and reduce privacy risks

Providing some flexibility in how privacy by design can be implemented, the article states that controllers can take into account 'the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'.

The second paragraph of Article 25 considers design by default, particularly the requirement for controllers to process only personal data necessary to the specific purpose of the processing, and ensure personal data is not automatically made available to third parties without the individual's intervention. This requires privacy settings, by default, to be as privacy-friendly as possible.

Privacy impact assessments

Privacy impact assessments (PIAs) are an integral part of taking a privacy by design approach. Essentially, they are a tool that can be used to identify and reduce the privacy risks of projects and reduce the risks of harm to individuals through misuse of their personal information. They can also support the design of more efficient and effective processes for handling personal data. An effective PIA will allow organisations to identify and fix problems at an early stage, reducing costs and potential damage to reputation.

Conducting a PIA involves working with people within the organisation, with partner

organisations and with data subjects to identify and reduce privacy risks. A successful assessment should benefit organisations by producing better policies and systems, and improving relationships between organisations and data subjects.

Data science and PIAs

The UK Government Data Programme has developed a Data Science Ethical Framework to help organisations understand the benefits and risks of using personal data when developing policy. The framework can be a useful tool if a project involves data science, Big Data or analytics. When conducting a PIA, the framework can be used as part of the process to help describe information flows and identify privacy risks and solutions.

Benefits of compliance

Implementing privacy by design and default can add a burden to the design of projects, processes, products and systems, but in many cases the upsides of compliance should outweigh the downsides. The benefits of a privacy by design approach include:

- Potential privacy issues can be identified at an early stage, making them simpler and less costly
- Awareness of privacy and data protection can be raised across an organisation
- Organisations are more likely to meet their legal obligations and less likely to breach GDPR
- Actions are less likely to be privacy intrusive and have a negative impact on individuals and therefore organisations

Data breaches and penalties

Introduction

GDPR introduces a more onerous and far-reaching regime around the notification of personal data breaches than the 1995 European Data Protection Directive, which contains no obligations to notify individuals of a breach, although some EU member states do have obligations to disclose breaches in regulatory guidance.

The regulation's focus on empowering data subjects and shaping behaviours through its enforcement regime means organisations must work hard to comply. Those that don't face risks of data breaches, draconian fines, reputational damage and, perhaps, collapse.

Personal data breaches

A personal data breach under GDPR is described in Article 4 as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. This includes breaches that are the result of both accidental and deliberate causes; affect the confidentiality, integrity or availability of personal data; and have a significant negative effect on individuals. A data breach is more than just losing personal data.

Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data that are lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

GDPR makes it clear that when a security incident takes place, organisations should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it. If a breach has occurred, the likelihood and severity of the resulting risk to individuals' rights and

freedoms, and potential negative consequences for individuals, must be established. If it's likely that there will be risk, the relevant supervisory authority must be informed, bearing in mind that organisations carrying out cross-border processing within the EU must determine a lead authority in the state where the organisation's central administration is located. If the breach doesn't need to be reported, it must be justified and documented.

A breach can have a range of adverse effects on individuals, including emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience, perhaps for those who need the data to do their job. Other breaches can affect individuals significantly and must be assessed on a case-by-case basis, looking at all relevant factors.

Once an organisation is aware of a personal data breach, it must act and be prepared for a lot of work in a little time, including:

- Identifying and resolving the point of failure or attack
- Gathering information relating to the factual, technical and legal background of the data breach
- Reporting to the supervisory authority
- Reporting to data subjects

Each of these points, independently and in combination, represent a potential area that could cause the downfall of an organisation.

Duty to report

The regulation introduces a duty on all data controllers and processors to report certain types of personal

GDPR Recital 85

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

data breach to their lead supervisory authority. Article 33 requires organisations to do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, organisations must also inform those individuals without undue delay.

To ensure compliance with these provisions, organisations need robust breach detection and investigation, which can be supported by data lineage and governance, as well as internal reporting procedures. This should help decision making about whether or not an organisation needs to notify the supervisory authority and affected individuals, and the sourcing of required information.

Information that must be reported to a supervisory authority when reporting a breach includes:

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of personal data records concerned
- The name and contact details of the data protection officer (if the organisation has one) or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the breach, including, where appropriate, measures taken to mitigate any possible adverse effects

Example of reporting

The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified to the supervisory authority, given the impact it is likely to have on individuals who could suffer financial loss or other consequences. On the other hand, it is not normally necessary to notify the supervisory authority, for example, about the loss or inappropriate alteration of an employee telephone list.

GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours and understand exactly what has happened and what mitigation is required. Article 34 allows required information to be provided in phases, as long as this is done without undue delay.

Individuals must be informed of a personal data breach if it is likely to result in a high risk to their rights and freedoms. Those concerned must be informed directly and without undue delay. A 'high risk' means the threshold for informing individuals is higher than for notifying a supervisory authority. The potential or actual impact on individuals as a result of a breach and the likelihood of this occurring must be assessed. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, the risk is higher.

In such cases, individuals affected must be promptly informed, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

If an organisation decides to notify individuals of a breach, it must also notify the supervisory authority unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. The decision-making process should be documented in line with the requirements of the accountability principle.

Information that must be provided to individuals in the case of a breach includes, in clear and plain language:

- The nature of the personal data breach

Example of reporting

A hospital suffers a breach that results in an accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and confidential medical details becoming known to others. This is likely to result in a high risk to the patients' rights and freedoms, so they would need to be informed about the breach.

- The name and contact details of the organisation's data protection officer (if it has one) or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, the measures taken to mitigate any possible adverse effects

Additional considerations

Article 33 of GDPR requires documentation of the facts relating to a breach, its effects and the remedial action taken. This is part of an organisation's overall obligation to comply with the accountability principle and allows supervisory authorities to verify compliance with notification duties under GDPR.

As with any kind of security incident, organisations should investigate whether or not a breach was a result of human error or a systemic issue and work to prevent a recurrence of the problem.

Failing to notify a breach when required to do so can result in significant fines and penalties, making it crucial to have data management processes in place that can support detection, reporting and access to the details of a breach.

Monetary fines and reputational damage

In pursuit of ensuring data protection, GDPR sets out numerous sanctions and corrective powers that can be used in cases of, or concerns about, non-compliance.

Monetary fines for non-compliance are astronomic, running up to €20 million or 4% of global annual turnover of the preceding financial year, whichever is higher. These fines are discretionary rather than mandatory, must be imposed on a case-by-case basis, and must be effective, proportionate and dissuasive.

There are two types of fines: fines of up to €10 million or 2% of annual global turnover, whichever is higher, in cases where data controllers or processors infringe their obligations, including data security breaches; and fines

of up to €20 million or 4% annual global turnover, whichever is higher, where individuals' privacy rights are breached.

Corrective powers include the ability to issue warnings to controllers or processors that intended processing operations are likely to infringe provisions of the regulation

When deciding whether to impose a fine and at what level, a supervisory authority must consider everything from the nature, gravity and duration of the infringement, to the intentional or negligent character of the infringement, action taken by an organisation to mitigate damage suffered by individuals, technical and organisational measures that have been implemented by the organisation, the types of data involved, and how the authority found out about the infringement.

The regulation also allows affected individuals to claim compensation for distress and damage caused by breaches and join class action suits against offending data controllers and processors.

The regulation's requirement to disclose breaches means they will be publicised and could cause controllers and processors significant reputational damage, as well as loss of customer loyalty.

Supervisory authority powers

Beyond imposing financial penalties, supervisory authorities have a range of disciplinary powers. Detailed in Article 58 of the regulation, these include investigative powers, including the ability to order data controllers and processors to provide any information required by the authority for the completion of its tasks, and to carry out investigations in the form of data protection audits.

Corrective powers include the ability to issue warnings to controllers or processors that intended processing operations are likely to infringe provisions of the

regulation, issue reprimands where processing operations have infringed the regulation, order compliance with a data subject's requests to exercise his or her rights, order the controller to communicate a personal data breach to the data subject, impose a temporary or definitive limitation including a ban on processing, impose administrative fines, and order the suspension of data flows to a recipient in a third country or to an international organisation.

Finally, supervisory authorities have authorisation and advisory powers ranging from providing opinion on the protection of personal data to national government, to authorising data processing if the law of a member state requires prior authorisation, and approving draft codes of conduct.

Failure to notify a data breach

Failing to notify a breach when required to do so can result in a significant fine of up to €10 million or 2% of global turnover. The fine can be combined with supervisory authorities' other corrective powers under Article 58. Firms need to have a robust breach reporting process in place to ensure they can detect and notify a breach on time and provide necessary details.

Outlook

Beyond compliance

On May 25, 2018, Europe's data protection regime will be transformed as General Data Protection Regulation (GDPR) goes live, putting the data privacy rights of individuals first and central, expanding on previous regulations and guidelines, and establishing draconian fines for data breaches that are driving compliance to the top of the regulatory agenda at many financial institutions.

Implementing the regulation is a large data management challenge requiring significant budget, IT involvement and human resource including lawyers and subject matter experts. It is also an evolution of data protection that will deliver benefits to both data controllers and data subjects.

Data controllers can look forward to operational benefits including reduced costs, fewer data locations, and improved data governance, as well as business benefits based on a better understanding of customers and including potential for product innovation and the ability to build customer trust, brand image and reputation.

Data subjects take control of their personal data and are able to find out what data is being held about them and how it is being processed and used. They also gain rights to request that their data is corrected or erased, and can apply to limit or stop data processing by controllers.

Sound results, but unlikely to be an early outcome of compliance as GDPR, like most regulations, will hit hurdles including interpretation, a shortfall of adoption by data controllers

processing data of EU citizens outside the region, and a rush of data access requests that could push data controllers to their limits.

Looking beyond these glitches to when the regulation's intent is realised, GDPR will harmonise data protection across the EU, provide a level playing field for data controllers and data subjects and, more broadly, push forward best practice data management across the financial sector.

Glossary

AML – Anti-Money Laundering

CSV files – Comma separated value files

Data controllers – Controllers determine the purposes and means of processing personal data; they are required to ensure contracts with processors comply with the regulation

Data processors – Processors area responsible for processing personal data on behalf of controllers

Data protection by design and default – also known as privacy by design and default

Data subjects – Individuals resident within the EU

DPIA – Data protection impact assessment

DPO – Data protection officer

EU – European Union

GDPR – General Data Protection Regulation

ICO – Information Commissioner's Office

KYC – Know Your Customer

MDM – Master data management

Personal data – Any information relating to an identified or identifiable natural person

PIA – Privacy impact assessment

Sensitive personal data – also known as special categories of personal data; categories include genetic data and biometric data where processed to uniquely identify an individual

CONSENT MANAGEMENT HEADACHES – SOLVED.

A consent management hub built on MarkLogic securely integrates and manages personally identifying information and consent data from siloed systems across your organisation – supporting GDPR compliance and new service innovations in one platform.

Get results in 30 days with our Quick Start service.

http://po.st/GDPR-Quick-Start · www.marklogic.com · sales@marklogic.com

MarkLogic®

Build your culture of compliance

Thomson Reuters Compliance Learning

Provide your employees with the tools to make the right decisions and protect your business from risk. Thomson Reuters Compliance Learning delivers engaging online training courses that cover a breadth of subjects. Our suite of data privacy courses will ensure you stay on top of the evolving regulations with topics including:

- GDPR in Daily Business
- Regional Data Protection Regulations
- Information Security Awareness

Learn more at risk.tr.com/compliance-learning

The intelligence, technology and human expertise you need to find trusted answers.

the answer company™
THOMSON REUTERS®