

Competitive Research



General Data Protection Regulation

JAN'2018

Content

Introduction	2p.
Snapshot GDPR Overview	4p.
Competitive Analysis	8p.
<i>Ernst and Young</i>	<i>8p.</i>
<i>PwC</i>	<i>15p.</i>
<i>Capgemini</i>	<i>18p.</i>
<i>Deloitte</i>	<i>24p.</i>
<i>KPGM</i>	<i>29p.</i>
Key Takeaways	34p.
References	36p.

Introduction

On May 25, 2018, the European Union's new data privacy regulations will go into effect. The new policy, known as General Data Protection Regulation (GDPR), has been in the works for over four years.

The legislation is designed to harmonize data privacy laws across Europe, protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. The new law marks a wide-reaching and significant shift in the way that organizations must protect personal data.

These regulations affect thousands of organizations around the globe - virtually any company that does business within the EU and holds personal data on EU residents.

It grants data subjects a number of new rights, including the right to judicial remedy against organizations that have infringed their rights, and requires organizations to adopt "appropriate technical and organizational measures" to protect personal data. It also introduces mandatory data breach reporting.

The EU General Data Protection Regulation provides the most comprehensive global framework.

Covered areas and topics

General provisions	<ul style="list-style-type: none">• Subject matter and objectives• Scope• Definitions		
Principles	<ul style="list-style-type: none">• Principles• Lawfulness of processing• Conditions for consent• Processing of special categories		Transfer <ul style="list-style-type: none">• Transfer with adequacy decision• Transfer by way of appropriate safeguards• Binding corporate rules• Derogations for specific situations
Rights of data subject	<ul style="list-style-type: none">• Transparency and modalities• Information and access• Rectification and erasure• Right to object and automated, individual decision making• Restrictions		Independent supervisory authorities <ul style="list-style-type: none">• Independent status• Competence, tasks, and powers• Activity reports
Controller and processor	<ul style="list-style-type: none">• General obligations• Security of personal data• Impact assessment• Data-protection officer• Codes of conduct and certification		Cooperation and consistency <ul style="list-style-type: none">• Cooperation• Consistency• European Data Protection Board Remedies, liability, and penalties <ul style="list-style-type: none">• Complaints and judicial remedies• Compensation, administrative fines, and penalties Specific situations <ul style="list-style-type: none">• Freedom of expression and information, public interest, scientific, historical research, or statistical purposes, etc.

Source: EU data-protection regulation 2016/679, Official Journal of the European Union, May 4, 2016, Volume 59, eur-lex.europa.eu

McKinsey&Company

On the other hand, according to IDC research GDPR has created a \$3.5 billion market opportunity for security and storage vendors. ⁽¹⁾

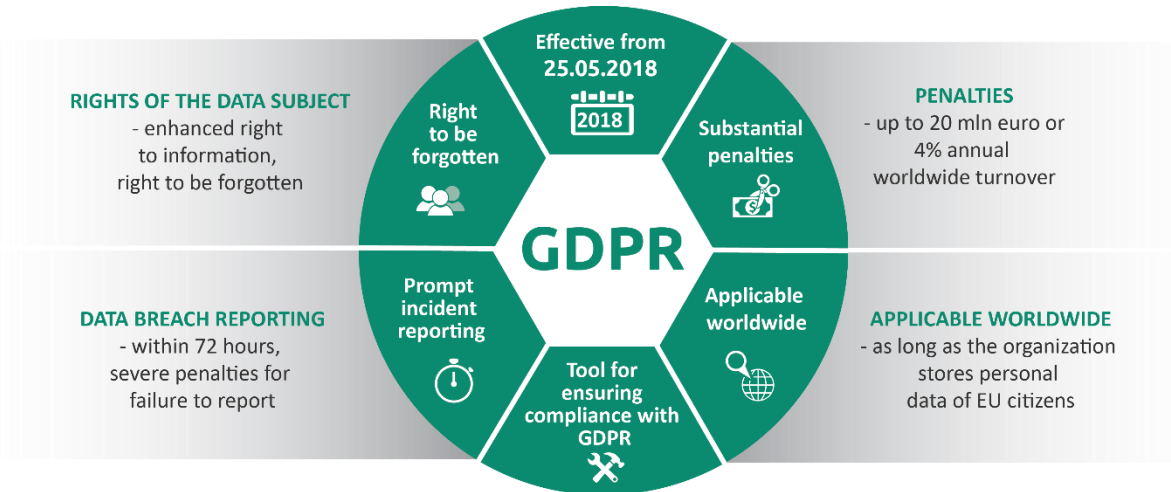
In this research paper, we will compare GDPR solution offerings from largest players on the market:

- Ernst and Young
- PwC
- Cap Gemini
- Deloitte
- KPMG

In the end, we will sum up our findings in Key Takeaways section.

Snapshot GDPR Overview

In this section, we will make snapshot GDPR overview, try to assess market opportunity created for IT service providers and evaluate readiness of companies to implement necessary changes.



The impact of GDPR is enormous and spans across a multitude of organizational areas:

Some of the key changes GDPR imposes include:

1. Increased Territorial Scope

- Any company processing personal data of subjects that reside in the EU must follow GDPR regardless of company location.

2. Consent

- Consent for data processing must be clear, distinguishable, and must be equally easy to give and withdraw.

3. Breach Notification

- In the case of any data breach, companies must notify all persons affected within 72 hours of becoming aware of the breach.

4. Right to Access

- Data Subjects must be given an electronic copy of the personal data free of charge.

5. Right to Be Forgotten

- Data Subjects now have the ability to requesting erasure of their personal data if certain criteria are met.

6. Data Portability

- Data Subjects have the right to receive personal data that concerns them.

7. Privacy by Design

- This concept has been around for years but now is becoming a legal requirement. It specifies that the data protection requirements must be considered from the onset of the designing of Info Governance and archiving systems.

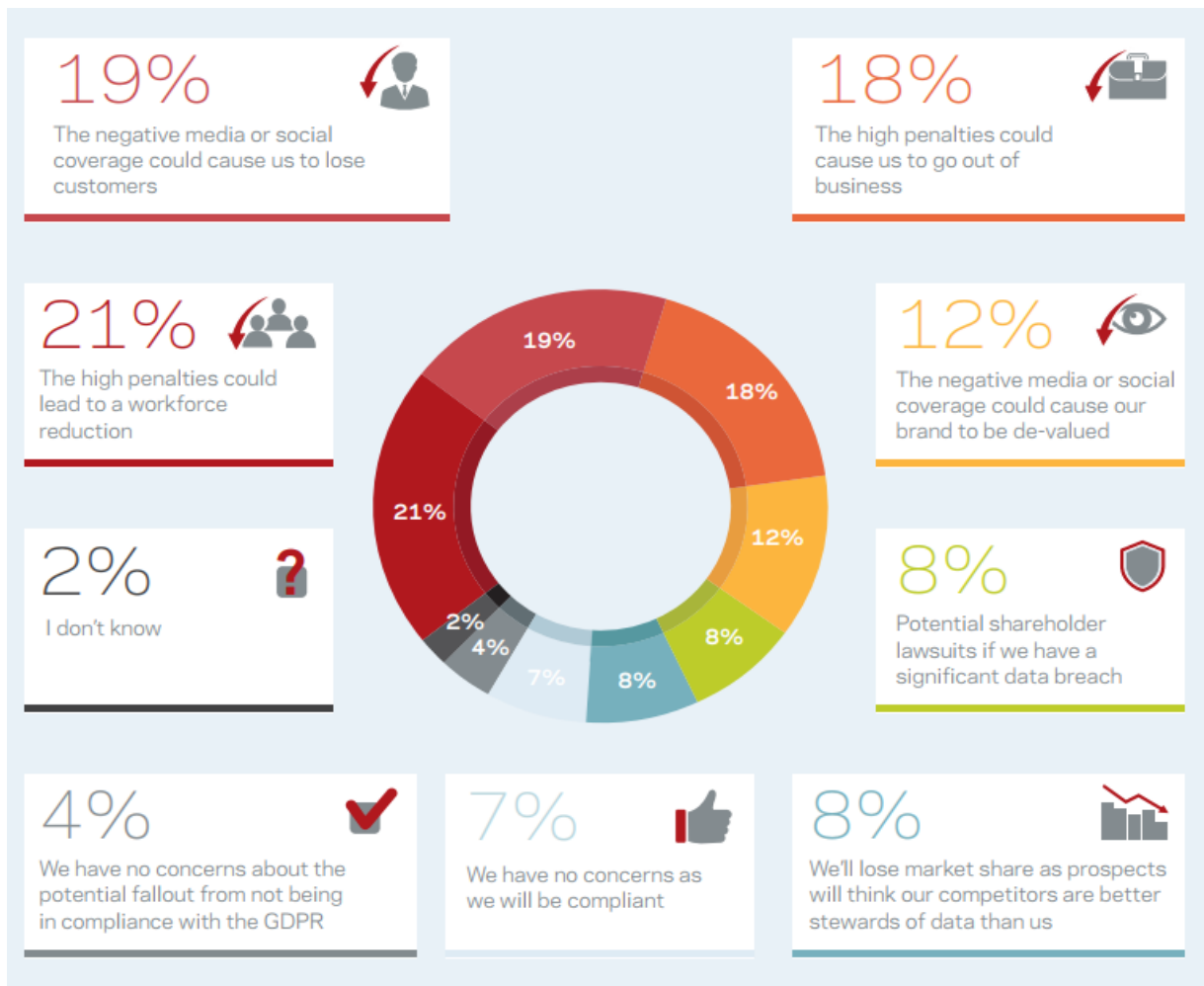
8. Data Protection Officers

- Controllers will have different requirements regarding Data Protection Officer meetings and regulations for communication regarding data processing activities. Any company over 250 employees will be required to have a DPO.

Any company that fails to follow the new regulations will face heavy fines or even dissolution. Fines are approached in a tiered way. Less serious compliance failures, such as an administrative failure in record keeping, face a fine of either 2% of annual global turnover or 10 million euros. Companies that have more serious offenses, including a breach of basic data protection principles, can be fined up to “4% of annual global turnover” or “20 million euros”, whichever is greater (see infographic).



Despite that fast approaching deadline, research commissioned by Veritas Technologies shows that 86% of organizations worldwide are concerned that a failure to adhere to the upcoming GDPR could have a major negative impact on their business. In addition, almost half (47%) of organizations fear they won't meet the requirements of the legislation, and many have critical concerns about what that could mean for their employees and their company as a whole.



Nearly two-thirds (65%) of respondents say that their organization has worked, or is currently working with, third parties to support their GDPR efforts. In addition, organizations are not afraid to assign a significant budget (albeit one that is still dwarfed by the size of potential fines for non-compliance) to support their GDPR readiness:

- On average, respondents expect their organization to have spent over one and a quarter million Euros (€1,360,567) or \$1,432,176 by May 2018 in order to achieve full compliance. ⁽²⁾

A separate Blancco Technology survey of more than 750 IT professionals found that 85% of Spanish companies, 77% of French companies, 73% of German companies and 65% of U.S. companies expect to spend up to \$3.99 million on GDPR-readiness technologies and processes. ⁽³⁾

Paul Hastings research found that firms listed in the FTSE 350 expect to spend £430,000 on technology and Fortune 500 companies expect to lay out \$1 million. However, only 10% of firms in the UK and 9% in the U.S. have purchased new technology before Oct-2017.

Technology aside, companies are budgeting for new hires to deal with regulatory issues. Of those polled, 40% of the FTSE firms have allocated from £201,000 to £400,000 for new permanent staff. In the U.S., 34% have set aside \$501,000 to \$1 million. ⁽⁴⁾

SAS survey found that: ⁽⁵⁾

- 45 % of organizations surveyed have a structured plan in place for compliance (but of those only 66% think that this process will lead to successful compliance) and 58% indicate that their organizations are not fully aware of the consequences of non-compliance
- Many organizations admit that they do not know how to determine if they are GDPR compliant
- Unsurprisingly, large organizations (5,000 employees+) are better equipped to handle GDPR with 54% being fully aware of the impact, compared to just 37 % of small organizations.
- Only 24 % of organizations make use of external consulting to become GDPR compliant, but those with a structured process in place use external consulting more often (34 %)

According to PwC findings: ^(6, 7)

- US companies lead their UK and Japanese counterparts in making steady progress in GDPR readiness
- Among all companies, 60% said they plan to spend at least \$1 million on GDPR preparation projects and 12% plan to spend more than \$10 million
- 77% of US companies plan to spend \$1 million or more on GDPR
- Over half of US multinationals say GDPR is their top data-protection priority
- Among executives polled in this survey, 69% said they plan to use a technology firm to help with their preparations, 62% plan to hire a consulting firm, and 46% plan to hire a law firm

According to research from RSM 92% of European businesses, not ready for GDPR. ⁽⁸⁾

From information above, we can conclude that:

- GDPR compliance is quite costly business (\$1-4 million)
- More than 25% of SMBs and up to 65% large enterprises will use third parties to support their GDPR efforts
- It creates great business opportunity for IT service providers which can offer GDPR solutions
- Large organization are better equipped to handle GDPR
- However, most businesses overestimate their GDPR readiness
- First five months of 2018 we will see big activity on the market as most organizations will try to be GDPR compliant before deadline
- Up to 80% of their GDPR allocated budgets will be spent during this period

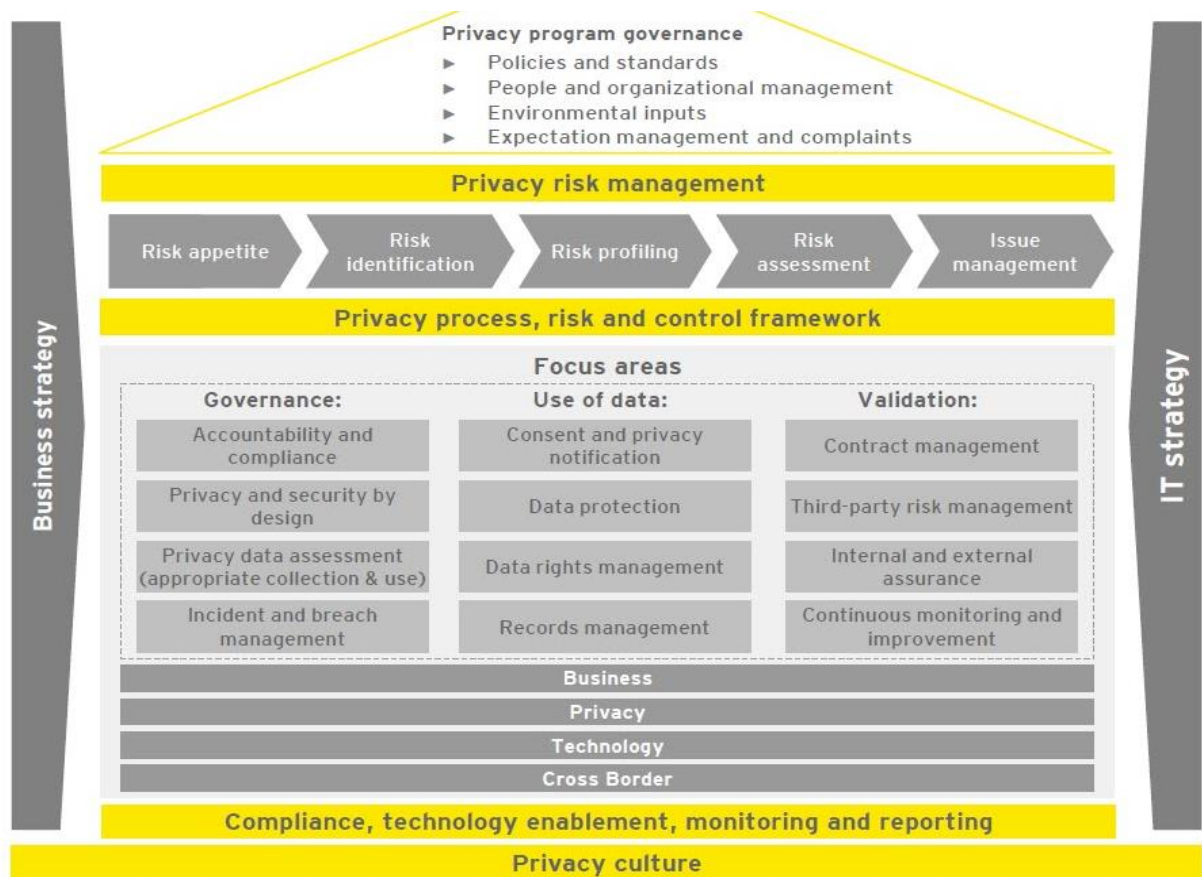
Competitive Analysis

In this section, we will compare GDPR offerings from key players.

Ernst and Young

GDPR Services/Deliverables

EY's privacy risk management framework:



Next steps

1

Educate key stakeholders, including the board of directors

2

Risk-assess to whether the GDPR applies to your organization

3

Establish cross-function and cross-business governance structure

4

Conduct a privacy impact assessment

5

Conduct a GDPR gap assessment

6

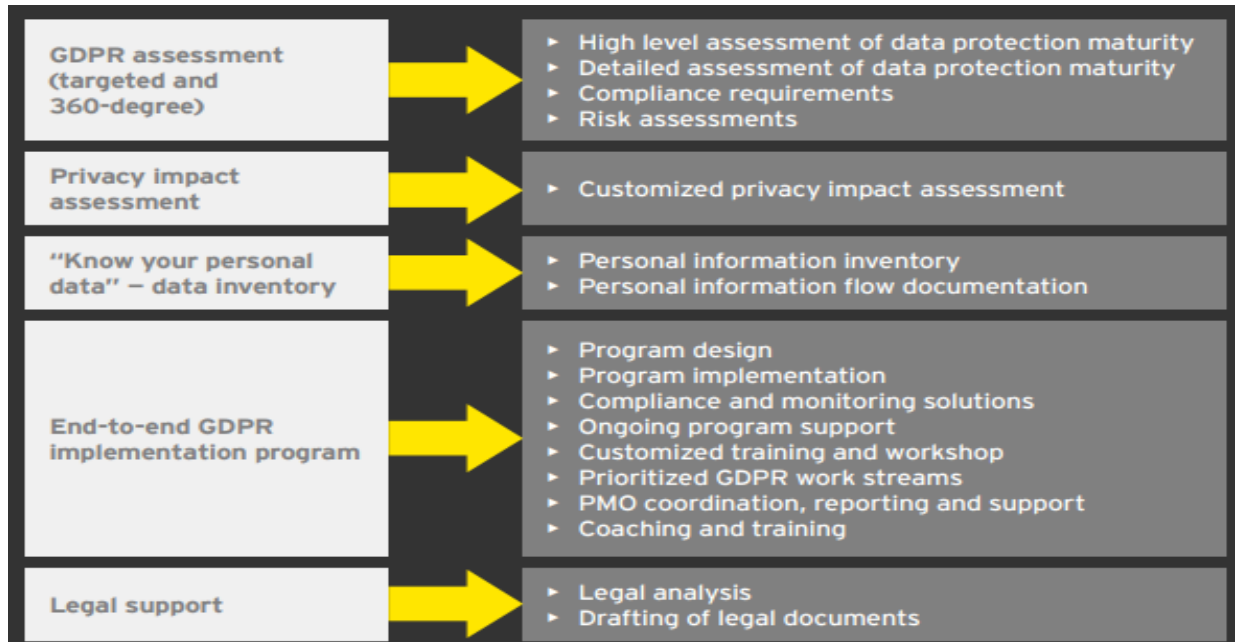
Design and execute a prioritized implementation plan

To support business stakeholder understanding of privacy, and the impact of the GDPR on business lines/functions, EY applied its privacy framework to the GDPR and categorized 12 focus areas into three themes, as shown in Table below.

	Focus area	Desired outcome
Governance	Accountability and compliance: privacy operating model, training/awareness, policy development	Creating structures and processes that enable proactive, systematic and ongoing compliance reporting for senior management
	Privacy and security by design: privacy impact assessment, program design based on business model	Achieving risk reduction and management through the application of requirements and tools integrated at various junctures in your process landscape
	Incident and breach management: data incident response plan, 72-hour operational effectiveness process	Enabling rapid management of a data breach, including internal investigations and external reporting
	Privacy data assessment: data use case management/framework, data classification, data flow mapping, data discovery, cloud discovery, high-value asset identification	Establishing and operationalizing governance over personal data usage and analytics as well as understanding the most meaningful attributes of your data that impact compliance risk and optimized use
Use of data	Consent and privacy notification: freely given and explicit consent, right to withdraw consent, privacy notices	Increasing transparency through explicit consent to process data and privacy notifications
	Data protection: identify and access management, technology selection, encryption strategy	Approach designed to achieve data protection and enhance your security hygiene
	Data rights management: data subject's right to access, correction, erasure, portability and/or objection	Empowering your organization to support data rights to access, deletion, portability and rectification
	Records management: attach requirements to physical files, electronic documents and emails	Strategy and program design that balances global privacy regulation with data protection, legal and business needs
Validation	Contract management: assessment of service-level agreements, assess internal or third-party contracts to identify gaps or identify opportunities to strengthen language	Discovery and revision of contractual provisions pertaining to privacy and security, including data permissions and restrictions
	Third-party risk management: third-party risk assessment, compliance monitoring and data controls	Understanding, designing and monitoring for the management of your third-party personal data access, protection, responsibilities and liabilities
	Internal and external assurance: internal audit assessment, third-party attestation, certification against industry standard	Providing independent confirmation that governance, risk management and internal controls as they relate to both privacy and security are designed and operating effectively
	Continuous monitoring and improvement: compliance monitoring program design, monitoring of key controls, dashboard reporting for management	Designing for ongoing awareness of privacy and security compliance to facilitate risk management and optimization of the control environment

*** - (9)

How EU helps organizations to prepare for GDPR implementation:

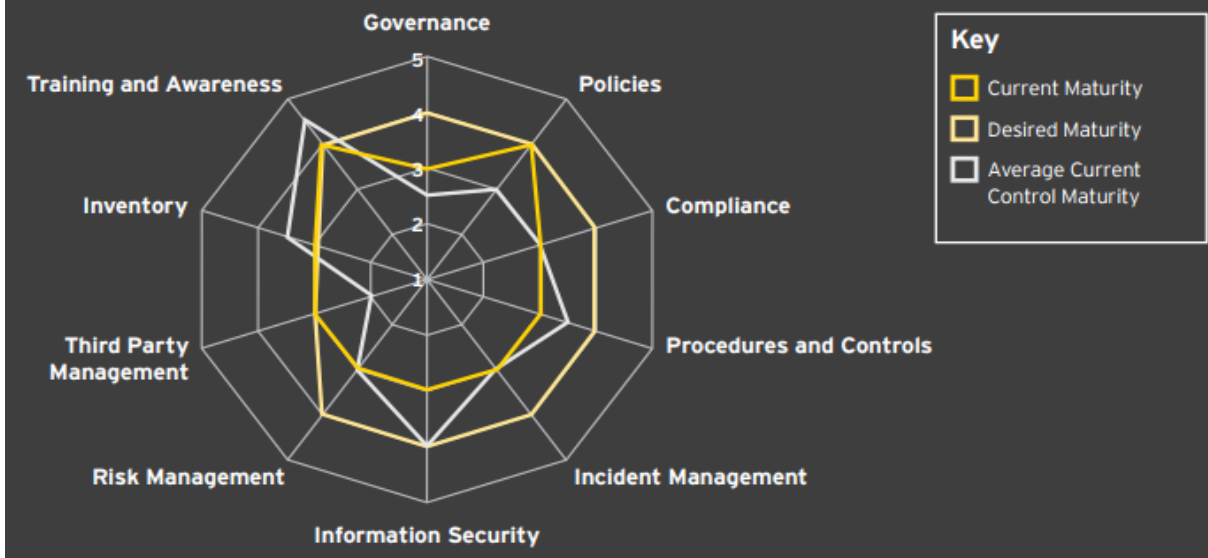


*** - (10)

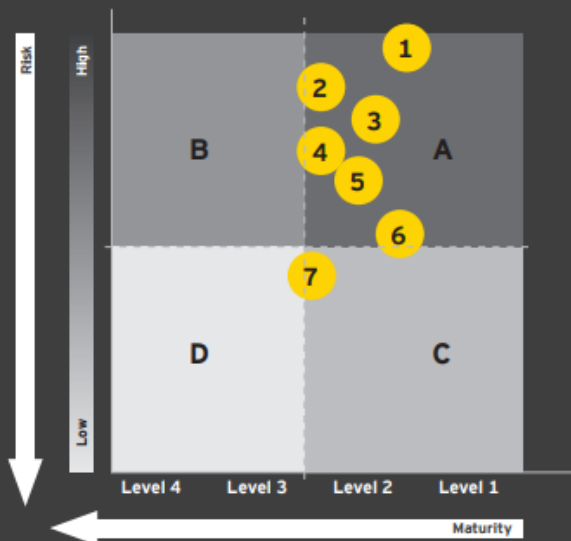
Solution	Overview	Service provider	Timescales
GDPR Targeted Assessment	High level assessment of data protection maturity	▶ Targeted assessment gauging readiness for the new requirements of the GDPR	1 day
GDPR '360 Degree' Assessment	Detailed assessment of data protection maturity	▶ Risk assessment and maturity evaluation based on industry framework and EU General Data Protection Regulation ▶ Recommendations and roadmap for remediation ▶ Product and process-specific risks	2-4 weeks depending on the size and complexity of the organisation
	Compliance requirements		
	Risk assessments		
Privacy Impact Assessment	Customised Privacy Impact Assessment	▶ Assessment of your systems or projects identifying key data protection risks	1-2 weeks depending on the size and complexity of the project or systems that need to be analysed
'Know your personal data' – data inventory	Personal information inventory	▶ Use of the Exonar Raven tool to identify and document a sample of the personal data you have in your organisation, where it is, where is transferred from/to, who has access to it ▶ Process or system specific personal information flow diagrams and documentation	2-12 weeks depending on the size and complexity of the organisation
	Personal Information flow documentation		

Solution	Overview	Service provider	Timescales
Data protection improvement programme	Programme design	Design and delivery of data protection improvement programmes, including the development and implementation of: <ul style="list-style-type: none"> ▶ Data protection frameworks ▶ Privacy governance and organisation design ▶ Policy and procedures ▶ Training and awareness ▶ Incident management ▶ Third Party management ▶ Risk management ▶ Procedures and controls ▶ Information security controls ▶ Binding Corporate Rules program compliance ▶ Ongoing compliance and monitoring 	3-24 months depending on maturity and size of the organisation
	Programme implementation		
	Compliance and monitoring solutions		
	Ongoing Programme support		
Legal Support	Legal analysis	<ul style="list-style-type: none"> ▶ Legal analysis of compliance with data protection legislation ▶ Drafting and advising on compliance programmes and policies ▶ Assessment of any non-compliance and suggestions of remedial action ▶ Drafting for data controller and data processor agreements ▶ Drafting of Binding Corporate Rules 	Assessed on a case by case basis - depending upon scope
	Drafting of legal documents		

We can work with organisations to enhance their understanding of their compliance position and maturity level. Below are some examples of the types of work products we have previously produced on data protection engagements:



Ey's risks map



Key

Circles

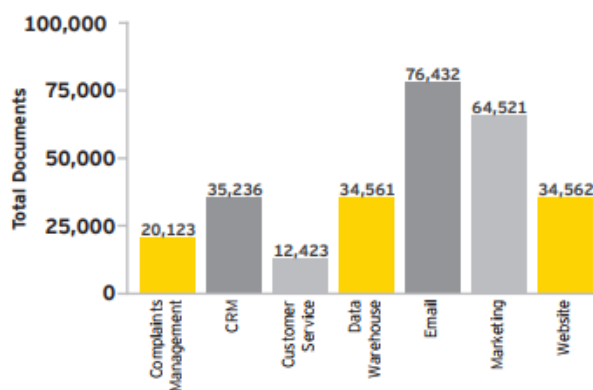
1. Third party management
2. Training and awareness
3. Risk Management
4. Policy
5. Data leakage
6. Treating customer fairly
7. Incident management

Sectors

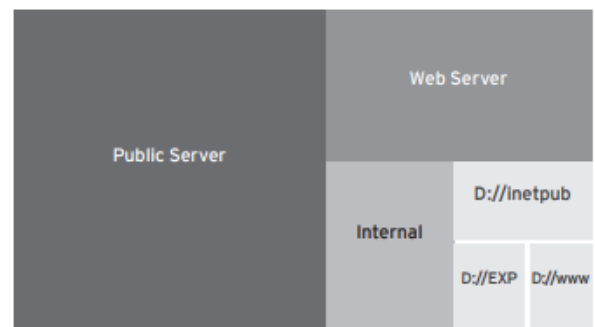
- A. Higher risk; Lower maturity
- B. Higher risk; Higher maturity
- C. Lower risk; Lower maturity
- D. Lower risk; Higher maturity

Organisations face many challenges preparing for the EU GDPR over the next couple of years. It is important that they understand their current state and the steps necessary to move towards compliance with the EU GDPR.

SPI/PII by Application System¹



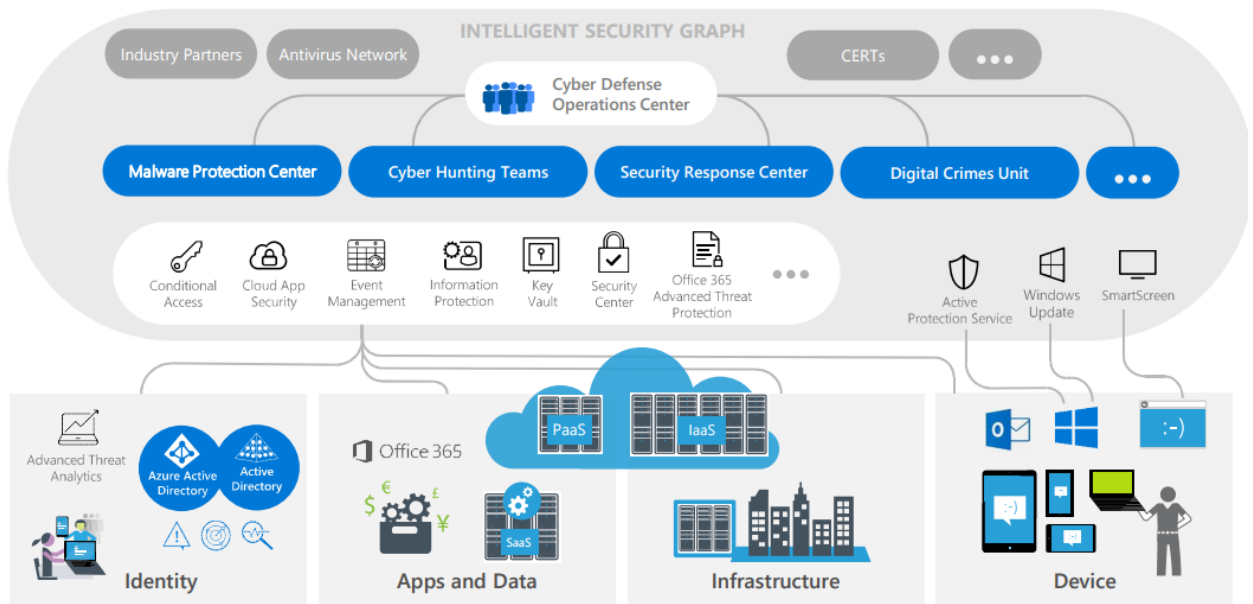
HR Data Located in Wrong Place¹



*** - (11)

EY to help businesses comply with EU GDPR in collaboration with Microsoft.⁽¹²⁾

Microsoft protecting you



*** - (13)





Pricing

We did not find in open web any mention of how much EY charges for their GDPR services. We think it depends on:

- Size of Organization
- GDPR gap (pricing will be determined after EY assessment)
- Industry

Contact People

We think pricing could be easily checked by direct contact. We identified the following people at EU responsible for GDPR implementation.

 <p>Erol Mustafa EMEIA Financial Services IT Risk & Assurance Leader Telephone: +44 20 7951 0700 Mobile: +44 7979 923 611 Email: emustafa@uk.ey.com</p>	 <p>Tony De Bos EMEIA Financial Services Data Protection & Privacy Leader Telephone: +31 88 407 2079 Mobile: +31 62908 4182 Email: tony.de.bos@nl.ey.com</p>
 <p>Philippe Zimmermann EMEIA Financial Services Legal Leader Telephone: +41 58 286 3219 Mobile: +41 79 341 4571 Email: phillppe.zimmermann@ch.ey.com</p>	 <p>Konrad Meier EMEIA Financial Services Data Privacy Professional Telephone: +41 58 286 4327 Mobile: +41 79 227 2367 Email: konrad.meier@ch.ey.com</p>

Americas

Cindy Doe

+1 617 375 4558
cynthia.doe@ey.com

Angela Saverice-Rohan

+1 213 977 3153
angela.savericerohan@ey.com

John Doherty

+1 212 773 2734
john.doherty@ey.com

Mark Watson

+1 617 305 2217
mark.watson@ey.com

Ed Keck

+1 216 583 1296
ed.keck@ey.com



Chris Gould

Partner, Cyber Security and Resilience

Tel: +44 20 7951 0086
Mobile: +44 7831 136 995
Email: cgould@uk.ey.com



Louisa Elder

Director, Head of IP and Data for Law

Tel: +44 20 7197 7929
Mobile: +44 7714 204 208
Email: lelder@uk.ey.com



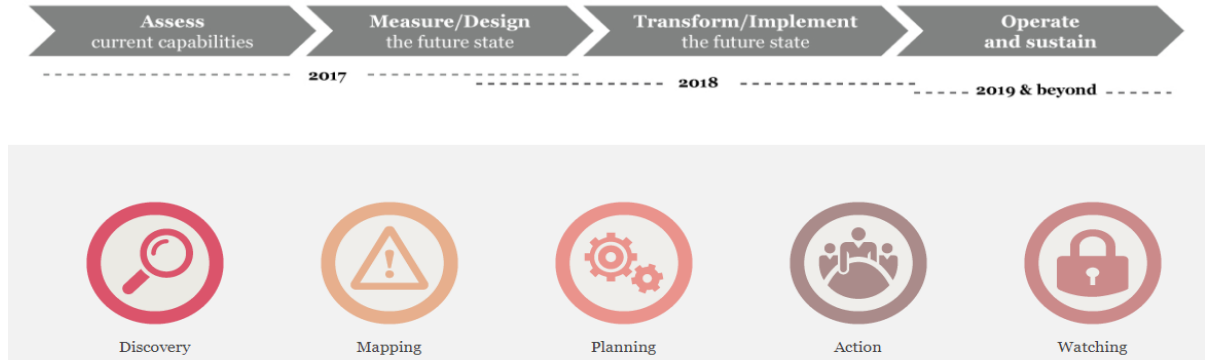
Nicola Hermansson

Director, UK&I Data Protection Leader

Tel: +44 20 7951 8332
Mobile: +44 7795 828 811
Email: nhermansson@uk.ey.com

GDPR Services/Deliverables

PwC GDPR program roadmap.



- **Conduct a readiness assessment**

Gather information to assess your organization’s current GDPR compliance maturity, and to help understand your critical legacy risks

- **Find remediation gaps**

Identify existing privacy capabilities and the work that needs to be done to bring your organization into GDPR compliance

- **Establish oversight**

Put your organization’s ongoing GDPR governance structure and model into place to coordinate and implement your remediation activities

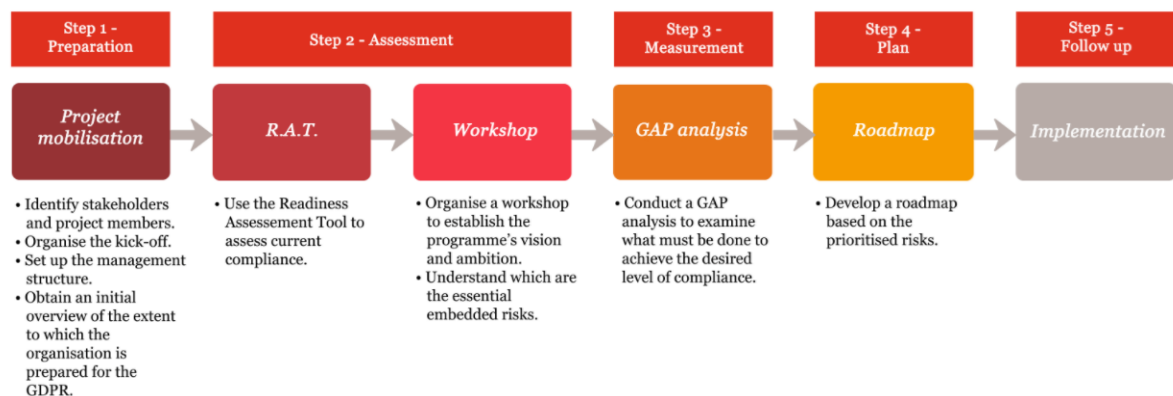
- **Implement your program**

Get your GDPR program off the ground: remediating gaps and establishing a privacy program

- **Conduct operation & monitoring**

Once GDPR is in effect and your program is in place, conduct ongoing compliance to drive continued accountability

The PwC approach:



As a whole, we found PwC GDPR solution offering is inferior to EY in scope and implementation. PwC is more focus on providing analytical reports, conducting surveys rather than practical part of business.

They have less branded technology partner – [Dathena](#).



Christopher Muffat, CEO at Dathena and Yan Borboën, Partner Cybersecurity at PwC

Nevertheless, we found one industry and country where PwC has edge over EY. It is financial service industry in Switzerland.

1	2	3	4	5
Understanding and Assessment	Strategy and Set-up	Design	Implementation	Operating (Run-the-Bank)
Assessment of the current data protection governance, compliance set-up and legal entities to ensure completeness	Development of an action plan and strategy set-up, including a project charter and project plan	Development of a risk assessment programme, amended data structure and change design	Ensuring a seamless integration of new designs for all applications and processes	Conduct a completeness assessment to ensure GDPR compliance
Develop data inventory to understand the full scope of data affected and assessment of data subject types	Outline implementation-roadmaps in consideration of the right legal paths, incl. third-party risk management	Create data flow diagrams of business processes and overview of flows between the business processes and applications	Amendments of contracts, where applicable, e.g. to receive consent	Establish/enhance data privacy training and awareness programme for employees
Analysis of the (i) data structure, (ii) IT architecture, (iii) process structure and (iv) data transfers	Define design principles for changes required and desired by the bank as well as definition of change priorities	Outline organisational changes where applicable	Implementation of new policy compliance programme and frameworks	Develop a communication plan for all relevant stakeholders and an incident response process for data breach cases
Screening and grouping of unstructured data supported by existing PwC tools Dathena and Online Collaboration tool	Analysis of data processing purposes and their legal grounds	Design of a fully automated data subject right management process	Implement risk management frameworks	Ensure an ongoing compliance assessment and completeness of the compliance framework
Analysis of products and services offered in order to understand what kind of data is collected/processed in which area	Analysis of required contract amendments, including third parties	Develop and design frameworks concerning the (i) management of privacy, (ii) roles & responsibilities and (iii) governance & reporting	Implement or amend data transfer flows and amend interfaces to third parties, where required	Establish an emergency plan for data breaches and other potential violations of GDPR

*** - (14)

In addition, PwC has strong GDPR teams in Australia and Netherlands. ⁽¹⁵⁾

Pricing

PwC GDPR pricing is individually tailored to needs of each organization and its current GDPR compliant readiness.

In order to receive PwC pricing idea it would be better to contact people indicated below.

Contact People

Jay Cline	Stewart Room
US Privacy Leader, PwC US jay.cline@pwc.com	Global Head of Cybersecurity and Data Protection Legal Services, PwC UK stewart.room@pwclegal.co.uk

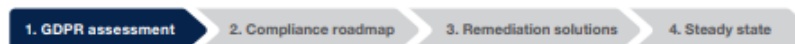
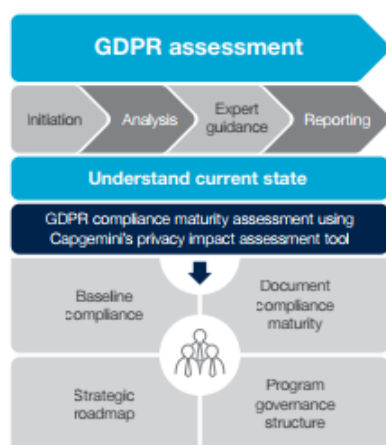
GDPR Services/Deliverables

Capgemini has very strong and comprehensive GDPR offering.

Capgemini's GDPR Methodology



1. Establish a baseline through GDPR assessment



The first phase is to undertake a GDPR assessment study that will:

- Establish the landscape of personal information captured, stored and processed;
- Evaluate the current maturity of information governance, security controls and associated privacy processes (e.g. Privacy Impact Assessment, Subject Access Request) across the organization; and,
- Evaluate the technical and operational maturity of the organization to meet the longer term requirements of GDPR and ensure a sustainable future state.

The starting point will vary according to the current level of compliance with existing regulation and the level of data privacy awareness for the organization. Using a proven impact assessment methodology and toolset already used across Europe, an initial baseline of data privacy maturity will be determined. Further detailed Privacy Impact Assessments will be undertaken driven by the gap assessment and associated risk.

2. Create a compliance roadmap



As a high-level view of the personal data landscape is established and the current level of compliance maturity determined, further detailed assessment and planning work is undertaken to create an overall compliance roadmap that:

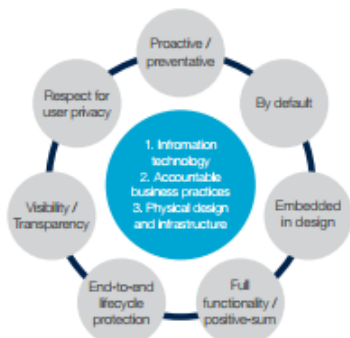
- Considers current controls and risk landscape (from a personal data perspective);
- Identifies a set of sub projects that your organization needs to execute to meet the compliance deadline in May 2018;
- Provides a view of the transition states for your organization's data landscape;
- Evaluates the current level of data governance implementation;
- Evaluates the technical framework supporting GDPR requirements.

This roadmap will also outline governance and delivery processes required to support execution of the roadmap (communications, scope, key stakeholders), the definition of the transition support function for the rollout of the GPDR projects, and indicative costs for the end-to-end delivery of the GDPR roadmap.

3. Implement remediation solutions



- Establish roles, responsibilities and clear accountabilities (e.g. DPO)
- Process definitions / revisions
- Develop GDPR compliance solutions (new and/or revised)
- Metrics capture & reporting



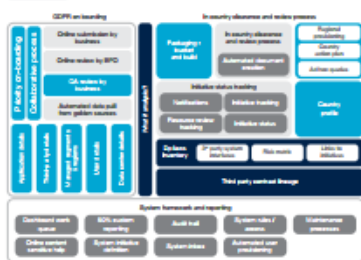
Driven from the findings of the assessment and the compliance roadmap, implementation and enterprise rollout of the required remediation solutions typically cover the following domains:

- Updates to organizational policies and governance– e.g. data privacy policies, data protection officer role, accountabilities;
- Definition/updates to key processes to support requests under individual rights (subject access request, erasure requests etc), embedding of privacy by design into existing processes as well as data protection impact assessments into system/process development methodologies;
- IT remediation solutions - Capgemini has a suite of solutions and accelerators from a range of vendors that include:
 1. **Information security** – data encryption, data erasure, database protection, breach protection
 2. **Information lifecycle management** – records management, data governance/data quality, data anonymization, information discovery, information archiving, analytics & reporting, data migration
 3. **Supporting solution accelerators** - case management frameworks (e.g. subject access request, breach notification/incident handling process), testing services, process redesign and governance framework
- Implementation change management – training and transition to business as usual privacy operating model.

4. Establish and sustain a steady state privacy culture and operational capability



- Monitoring and measurement – centralized reporting
- Processing register (by risk type)
- Remediation activities workflows
- Measure outcome using standard metrics



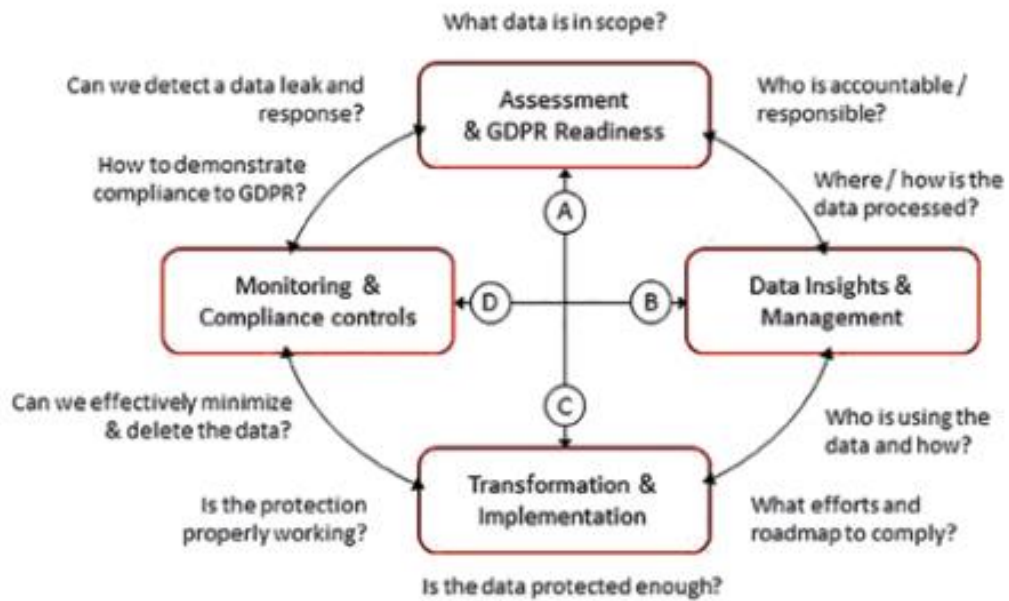
Critical to the long term success of any remediation implementation is to ensure that the changes are sustainable and maintainable for the future. Experience has demonstrated that the operational effectiveness can only be sustained with:

- Monitoring of key privacy-related metrics – staff training, PIAs, individual rights requests, incidents/near misses, key controls;
- Maintaining a view of personal data being processed as the business and systems change, through a well governed and managed processing register;
- Embedding key principles (e.g. privacy by design) into any new system/process workflows;
- Continuous improvement on policy, risk assessment, controls and the approach to measuring and managing their design and operational effectiveness.

*** - (16)

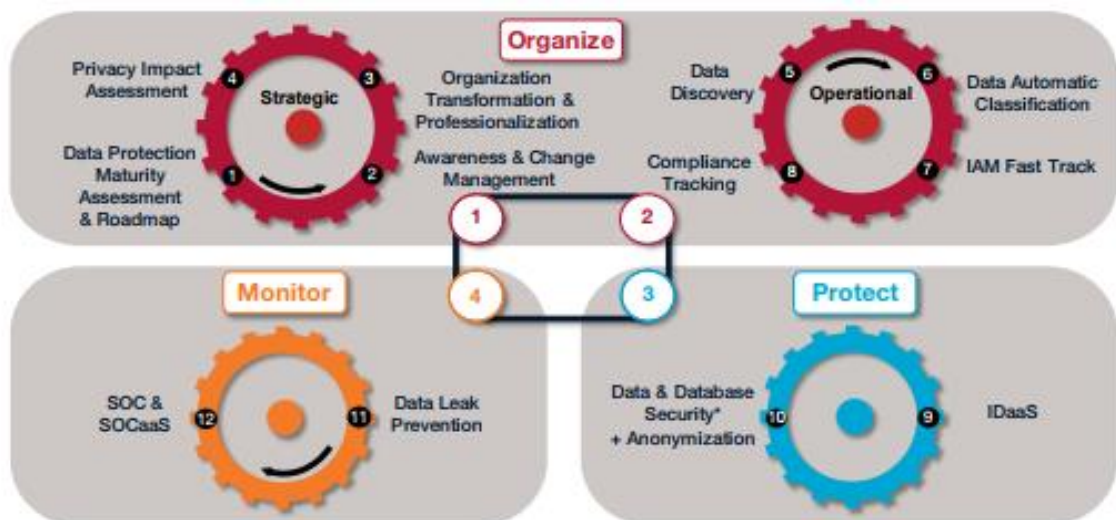
Capgemini offers 12 specific services to help organizations to comply with GDPR:

Simplified Portfolio	Our 12 Services	
Assessment & GDPR Readiness	• Maturity Assessment & Roadmap	• Identity & Access Management "FastTrack"
Data Insights & Management	• Data Discovery & Data Classification	• Data Protection Impact Assessment
Transformation & Implementation	• Awareness & Change Management	• Database security
	• Organization Transformation & Professionalization	• Unstructured data security
		• Identity & Assess Management (IDaaS)
Monitoring & Compliance Controls	• Compliance Tracking	• SOC & SOCaS
	• Data Leak Prevention	



Their Consulting and Data Management services will help organizations answer six key questions:

- What data is in scope?
- Where and how is it processed?
- Who is using it and how?
- Who is accountable / responsible?
- How is it collected, minimized and deleted?
- What effort and roadmap to comply?



*** - (17)

Capgemini has strong technology partners in GDPR implementation- Oracle and SAP.

GDPR technology solutions

Capgemini proposes the project management, and Oracle the technical implementation, of three technology solutions which are applicable to existing, legacy and new digital systems:

- Database Security options, best solutions to secure the Oracle DB (Oracle on Oracle), such as Advanced Security and Key Vault, Database Vault, Audit Vault and Database Firewall, Database Masking and Subsetting and Label Security.
- Identity and Access Management, to manage the opportunity given by the digital transformation, such as Identity Governance, Access Management, Directory, Identity Cloud Service and API Platform Cloud Service.
- High availability and resilience solutions, an area where Oracle has achieved the excellence since many years, with products like Exadata, Real Application Cluster and DB Recovery Appliance to name a few.

In our experience, an early start towards GDPR readiness is critical. May 2018 is closer than most realize. GDPR can have a significant impact on the business processes of your organization and therefore GDPR readiness cannot be achieved overnight. Our combined set of offerings ensures readiness for GDPR, as well as improved risk mitigation. Additionally, readiness for GDPR improves your overall data management, which in turn will protect your assets.

*** - (18, 19)

Implementation cases:

Example 1: large European bank

The first organization is a large European bank. The bank is working towards GDPR compliance and considers readiness as a means to underscore trust and security. Senior management has consulted a specialized law firm and its technology partners. Senior management understands the implications of the GDPR. The bank drafted a road map to achieve GDPR readiness and appointed a DPO in 2015 even before the approval of the new law. The bank has modified its applications, portal and processes to give clear information to its customers and to collect different degrees of consent about usage of personal data. The organization understands how to address the GDPR holistically in the context of the many other regulations it has to comply with. Also, Data Protection has been integrated into the Information Security Management System (ISMS) of the bank.

Additionally, it has adopted an internal communication strategy that explains the need for its new measures. The DPO has helped identify all applications that process personal data and all databases containing personal data. The bank strives to avoid – at all cost – the loss of personal data. However, on two occasions a data breach was reported. Processes geared towards mitigation and recovery ensured that the breaches were addressed quickly and the consequences were minimized. Additionally the bank promptly reported the breaches to the required authorities and the affected clients according to the predefined procedures. The bank has worked with Capgemini and Oracle to build a plan for readiness. The execution of the plan ensures readiness of its staff, organization, processes, infrastructure and IT for the GDPR.

Example 2: large car manufacturer

The second organization is a large car manufacturer. The manufacturer associates GDPR compliance with its valuable brand image, which is key to the organization and is therefore keen on getting GDPR right. The car manufacturer had adopted a new strategy where big data and analytics serve as the cornerstones of their plans, leading them to increasingly using and producing an abundance of data. Although the car manufacturer has appointed a DPO and has set-up elaborate awareness campaigns on data and protection, the vastness, technical complexity and international character of its data and database landscape is becoming increasingly complex. Although the car manufacturer is unwilling to accept risk, its data protection and data experts know that the GDPR and future data breaches spell fines from the EU – which may harm brand image and lead to an unacceptable loss in fines. The car manufacturer works with Capgemini and Oracle to implement solutions to further increase database security, identity and access management and resilience solutions

Example 3: family owned national retail organization

The third organization is family-owned national retail organization of 300 small and mid-size supermarkets in Western Europe. Its senior management is not aware of the GDPR and no measures have been taken that are geared towards compliance. The organization has never dealt with significant data breaches, although it has been collecting personal data from its clients since 2005. The retailer uses the data for digital marketing and online shopping. The retailer does not have a DPO in place and does not link data protection or security to its core business. Its landscape of applications and associated databases has not been checked for personal data. In short, the leadership of the organization has not considered data protection and security and is not yet ready to deal with data breaches. The retail organization had turned to Capgemini and Oracle for an analysis and recommendations on planning, governance, process, culture, data and technology with the aim to test readiness for GDPR.

Their portfolio considers the most important topics for executives regarding data protection and security. Their portfolio consists of four categories: ⁽²⁰⁾

- GDPR assessment (Duration 2-3w)

The assessment is an analysis and recommendations on planning, governance, process, culture, data and technology. The result of the assessment is a list of categorized findings, conclusions and actionable recommendations that aim to prepare for the GDPR. The assessment may be the first step towards implementation of other categories, such as planning, governance, process, culture, data and technology. The assessment may also confirm that all preparations are in place.

- GDPR strategic plan (Duration 2-4w)

Capgemini can help to include a set of defined action items that employ the use of technology to raise the quality and level of personal data protection within your organization into your strategic GDPR plan. The stakeholders from your organization will be involved in creating a realistic, supported, and actionable plan. Capgemini will facilitate by utilizing its experience with strategic plan development, GDPR readiness capabilities and gained insight into your business and technology solutions

- GDPR data protection impact assessment (Time frame dependent on size)

Capgemini will help to assess the GDPR readiness of your IT infrastructure for any type of processing. At the start, a data protection impact assessment scope, governance, questionnaire and tooling are tuned to the specific needs of your organization. To ensure cooperation of all target groups, an awareness campaign on GDPR and data protection is initiated. A selection of relevant information systems is made based on their initial data protection risk. Based on the answers given in the data protection impact assessment tool, the impact of each system is calculated and an overview of gaps, risks and measures is generated. The tool provides a dashboard with gaps for each role, risks scores and mitigating measures which are categorized. Subsequently, a consolidated internal (board) and external (regulator) report can be generated. The results provide the starting point for an improvement plan for the Data Protection Officer

- GDPR technology solutions (Time frame dependent on approach)

From information above, we can conclude that on average Capgemini completes GDPR implementation within 3-6 months.

As we pointed out above Capgemini has very strong and comprehensive GDPR offering. Its stronghold is Europe.

On the other hand, we found that the company does not have strong GDPR implementation team in North America.

Pricing

Similarly, to EY and PwC mentioned above Capgemini set pricing only after GDPR assessment. We estimate that only in Europe their GDPR services revenue stream exceeded \$25 million in 2017. It means that their GDPR client portfolio there exceeded 20 organizations.

Contact People

Lee Smith
GDPR and ECM, Capgemini UK
lee.c.smith@capgemini.com

Data Governance: **Graham HUNT**
Director - Insights & Data Practice
graham.hunt@capgemini.com

John Horton
GDPR, Capgemini UK
john.horton@capgemini.com

GDPR Global Lead: **Pierre-Luc REFALO**
Global Head of Cybersecurity
Strategic Consulting
pierre-luc.refalo@capgemini.com

Data Protection: **Maxwell KEYTE**
Leader CyberSecurity | Capgemini AppsTwo
maxwell.keyte@capgemini.com

GDPR Services/Deliverables

Deloitte predictably has strong GDPR offering. The company put talent availability in the space as one of their key their strengths: (21, 22, 23)

- More than 12.000 IT risk consultants and 3,000 security professionals worldwide
- More than 1.400 global and privacy practitioners
- From which 180+ in UK and 175+ in EMEA

Deloitte accreditations	
ISC ²	Over 1,100 CISSPs
ISACA	Over 2,000 certified as CISA, CISM, CGEIT
BSI	Over 150 trained lead system auditors
IAPP	Privacy certified practitioners
Specialty	Wide range of domain specific certifications
PMI	PMI certified practitioners

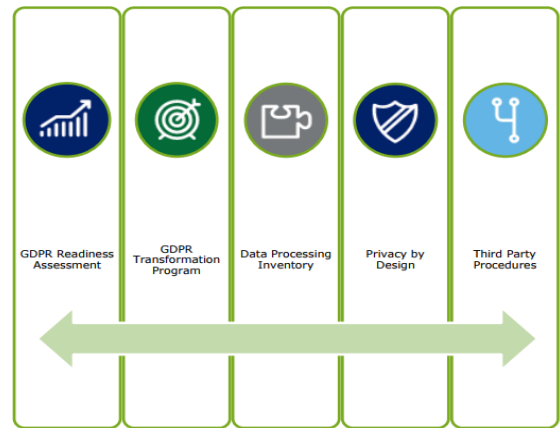
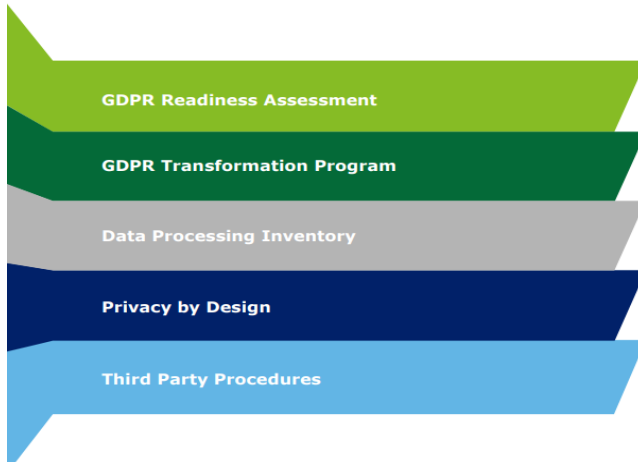
Besides, they boast that Gartner Deloitte ranked #1 in Security Consulting for the fifth consecutive year. (24)

However, some experts dismiss this claim and state that Deloitte inflated its security revenue number by a factor of at least 450%, principally by counting whole deals that include security elements. Besides, they say that Deloitte was already regarded as 'problematic' in its role of technology implementation services firm inside industry with many reported project failure cases. (25)

Deloitte GDPR services

Compliance and Readiness	Privacy Programmes	Technology and Digital	Risk Management	Training and Cultural Change	Cyber Security
<ul style="list-style-type: none"> •GDPR readiness assessment •GDPR compliance roadmap •Global privacy compliance assessment •GDPR technology impact assessment •Global compliance assessments 	<ul style="list-style-type: none"> •Privacy programme development •Privacy strategy and roadmap development •Target operating model design and implementation •Change programme design and delivery 	<ul style="list-style-type: none"> •Data discovery, mapping, and inventories •Privacy-by-design advice and application •Online and e-Privacy •Digital asset risk assessment and management (e.g. websites and mobile apps) 	<ul style="list-style-type: none"> •Privacy Impact Assessment and health check •Policy analysis and design •Governance and compliance review •Third party management •Mergers and acquisitions data transfer and ownership 	<ul style="list-style-type: none"> •Privacy risk and compliance training •Training and awareness design and implementation •Classroom and computer-based training •Cultural change programme development 	<ul style="list-style-type: none"> •Personal data breach investigation and management •Regulatory liaison advice •Incident response and forensic investigation support •Supplier and third party management
<p>We have experience with performing assessments of organisation's readiness based on GDPR requirements, among others.</p>			<p>We designed and developed a group-wide privacy programmes for a consumer business clients.</p>		
<p>Our deliverables help organisations to gain a better insight in their processes regarding privacy, such as: formal reports, governance models, policies and processes, and roadmaps.</p>			<p>We supported the cyber response for a consumer business client which had suffered hacking and a data breach, providing advice on their customer notification and regulatory obligations.</p>		

Actions to take to prepare for the GDPR



GDPR Readiness Assessment

The road to GDPR compliance with the GDPR Maturity Assessment & Roadmap

What is the GDPR Readiness Assessment?

To give a clear picture on where your organization currently stands with respect to the GDPR, the GDPR Readiness Assessment is the tool of choice. The GDPR Readiness Assessment is:

- A powerful tool, based on an existing Deloitte platform to create a baseline for privacy;
- Part of the cyber tooling suite, potential to incorporate into your broader cyber strategy and roadmap;
- Used by Deloitte globally for privacy and cyber assessments and strategy definition;
- A good starting point for becoming compliant with the GDPR and getting a tailored privacy program;
- Based on our Privacy, Security and Governance framework, covering all elements of the described privacy program;
- Instrumental in finding the areas with the biggest risk;
- Used to focus on those areas which most urgently need action to become GDPR compliant;
- A method to measure how mature the organization currently is, using the Deloitte privacy and data protection maturity model.

1. Capture Business insight

Privacy compliance & GDPR Readiness framework tailored based on industry and organizational characteristics.

2. Insight in current privacy situation

A thorough assessment by workshops and interviews with (a part of) the organization, giving insight of the current level of maturity against the framework.

First steps in becoming GDPR compliant

Our maturity approach to privacy challenges is based on industry best practices, Deloitte advisory methodology and our experience with privacy and cyber engagements at a large number of other clients. Deloitte has conducted a number of relevant benchmarks over the years, such as the Privacy Benchmark and the Governance Benchmark, which can be referenced to determine your organization's current standing.

3. Develop Strategy & Roadmap

A practical and concrete roadmap with prioritized steps required to improve, risk-based, the state of privacy compliance with the GDPR.

Privacy by Design

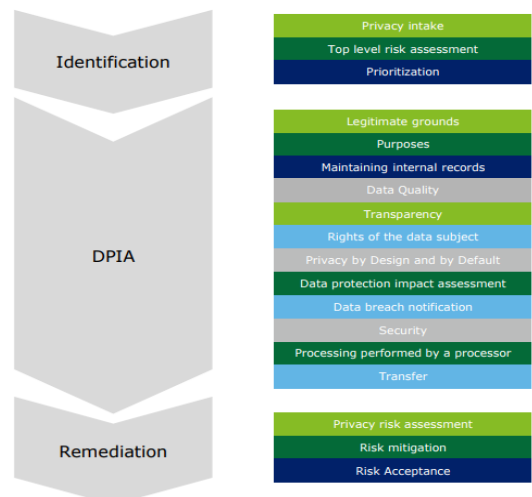
Embedding privacy into your project methodology by assessing privacy risks in an early stage

A tailored approach

Privacy can be considered as an operational risk that requires practical solutions in order to make sure that risk is actually handled. The challenge is to provide uniform and flexible methodologies and process to safeguard privacy every time a data driven project starts.

Key elements to consider

- Ensuring new projects and initiatives abide by the privacy rules within your organization is done through a robust Privacy by Design (PbD) approach;
- Data Protection Impact Assessments (DPIAs) are based on the GDPR and are a proven and effective tool to assess privacy risks;
- A PbD approach consists of a number of elements: a PbD process, DPIA method, and a remediation framework:
 - The **DPIA process** describes the phases of identification, DPIA and remediation covering roles, responsibilities, sign offs, escalation, support for a DPIA and should be efficient and effective;
 - A **DPIA method** is the combination of checks, questions and requirements to assess the impact and risks that any system or project should follow;
 - **Remediation** should always be the end phase of privacy by design and makes sure impact can be reduced and risks mitigated or accepted.

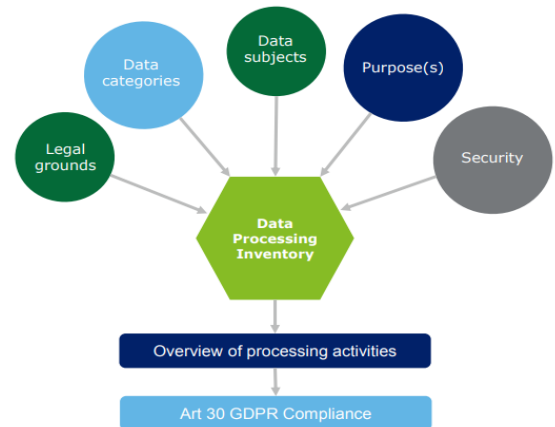


Data Processing Inventory

Creating a data inventory provides an overview of all data and insight in the risks attached to processing activities

A Data Processing Inventory is your basis to get in control of your data processing

- A data inventory is an overview which includes all the required information concerning personal data processing, such as legal grounds, purpose(s), categories of data, retention period and conducted risk analysis.
- Having an inventory is an actual requirement under the GDPR (following from article 30), but it can also serve you well in building your understanding of the personal data you processes.
- The inventory is used as a register of all the data processes within the organization. Having an inventory is essential for your oversight of processing activities and is a mandatory element of GDPR compliance.
- The inventory allows your organization to demonstrate awareness of its obligations as a data controller, including keeping of records of processing activities.
- Finally, knowing which personal data the organization processes mitigates the risk of unidentified data breaches.

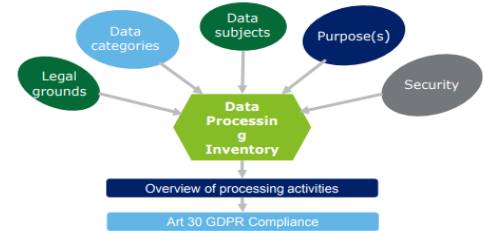


Data Processing Inventory

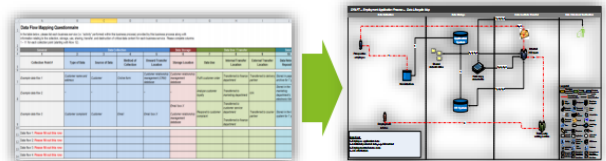
Creating a data inventory provides an overview of all data and insight in the risks attached to processing activities

A Data Processing Inventory is your basis to get in control of your data processing

- A data inventory is an overview which includes all the required information concerning personal data processing, such as legal grounds, purpose(s), categories of data, retention period and conducted risk analysis.
- Having an inventory is an actual requirement under the GDPR (following from article 30), but it can also serve you well in building your understanding of the personal data you processes.
- The inventory is used as a register of all the data processes within the organization. Having an inventory is essential for your oversight of processing activities and is a mandatory element of GDPR compliance.
- The inventory allows your organization to demonstrate awareness of its obligations as a data controller, including keeping of records of processing activities.
- Finally, knowing which personal data the organization processes mitigates the risk of unidentified data breaches.



In data mapping, there are two stages: the data capture template and the data map flowchart.



Data capture template

Data Map flowchart

Third Party Procedures

External parties bring specific challenges for data controllers

Data Breach Handling Procedure

When a data breach occurs there are many internal and external challenges. Handling and communication procedures with processors, authorities and data subjects are essential for effective data breach handling.

Data Processing Agreements (DPAs)

Are your DPAs GDPR proof? With the new data breach rules in place there is a requirement for contractual arrangements between Controller and Processors.

Vendor Assessment

Every time your organisation uses a third party for any kind of service that might involve data processing there should be a concrete process with clear requirements to assess these parties and their specific service.

To make sure this is done effectively there needs to be collaboration between legal, risk, IT and procurement with strong steering from the DPO.

Data Subject Rights procedure

The most important external stakeholder are your data subjects. The GDPR brings increased rights to data subjects (customers, patients, citizens) and this brings procedural challenges to a controller. Whether a data subject requests access, erasure or portability of their data, a good process on how to communicate and serve these data subjects is essential.

Deloitte technology partner in GDPR implementation is Canadian firm Ataccama Corporation. ⁽²⁷⁾

Implementation cases:

Our team performed an assessment of a pharmaceutical organisation's readiness with key GDPR requirements, issuing a formal report and prioritised compliance roadmap.

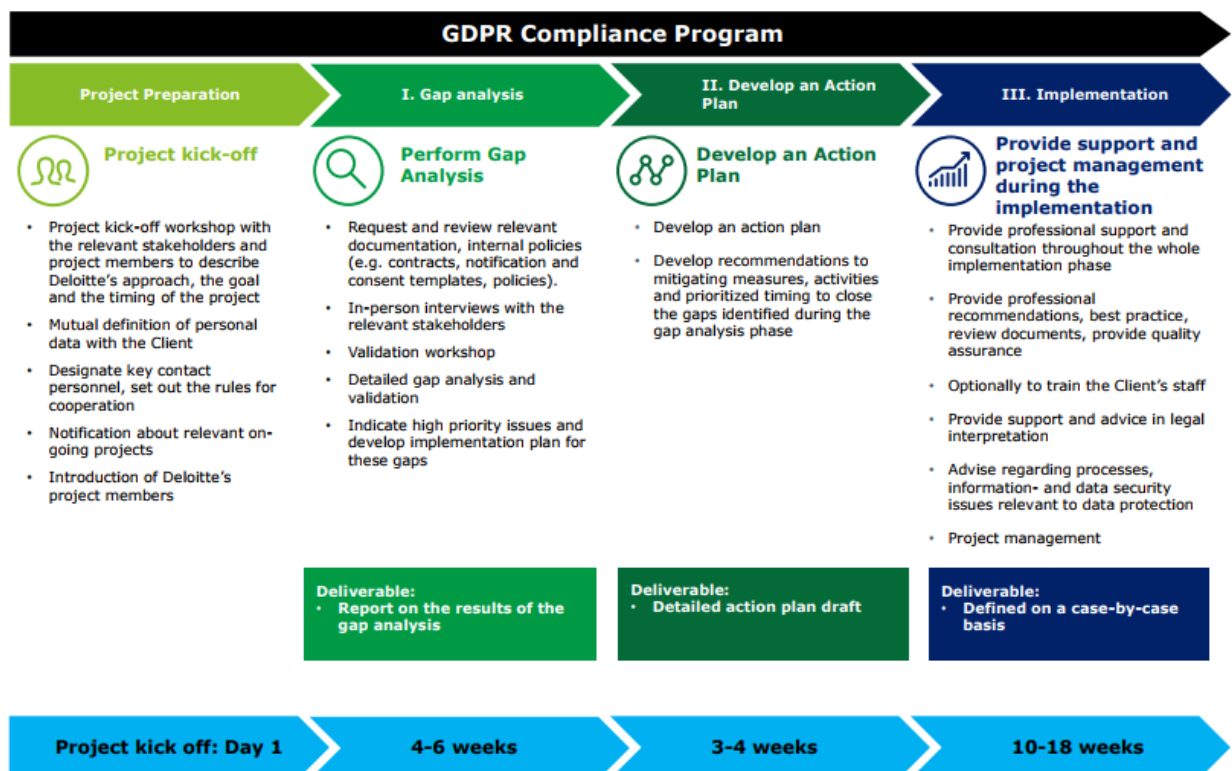
We designed and established a new privacy function for a global financial services organisation, creating a governance model, policies and processes, and bespoke privacy training.

We designed and implemented a group-wide privacy programme for a consumer business client, and delivered a gap analysis, a PIA procedure, policies, and a privacy operating model.

We supported the cyber response for a consumer business client which had suffered hacking and a data breach, providing advice on their customer notification and regulatory obligations.

*** - (28)

From graph below, we see that GDPR implementation process offered by Deloitte takes minimum 3-months.



*** - (29)

Pricing

We did not find any references of Deloitte GDPR services pricing on open web sources. However, we think the company pricing is in line with main competitors in the space.

Contact People

The Netherlands



Annika Sponselee
Partner | Deloitte Privacy Services

Deloitte Risk Advisory
Gustav Mahlerlaan 2970
1081 LA Amsterdam
The Netherlands
+31 (0)6 1099 9302
ASponselee@deloitte.nl

United Kingdom



Peter Gooch
Partner | Deloitte Cyber Risk Services

Deloitte Risk Advisory
Hill House 1 Little New Street
London, EC4A 3TR
United Kingdom
+44 7803 003849
pgooch@deloitte.co.uk

Switzerland



Erik Luysterborg
Partner | Deloitte Cyber Risk Services

Deloitte Risk Advisory
Gateway Building Luchthaven Nationaal 1 J
Zaventem, 1930
Belgium
32 497 51 53 95
eluysterborg@deloitte.com



Ed Powers

US Managing Principal | Cyber Risk
Services Leader

epowers@deloitte.com

+1 201 499 0605

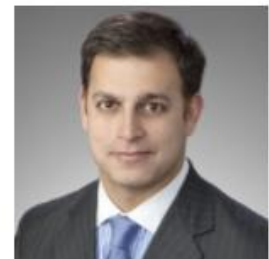


Emily Mossburg

Principal | Deloitte Risk and
Financial Advisory

emosburg@deloitte.com

+1 571 766 7048



Adnan Amjad

Partner | Deloitte Risk and
Financial Advisory

aamjad@deloitte.com

+1 713 982 4825

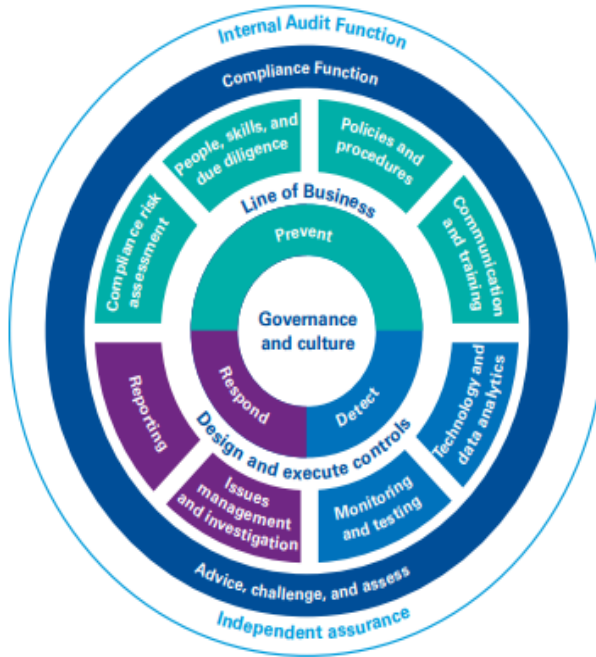
GDPR Services/Deliverables

Organizations are faced with a multitude of challenges when evaluating GDPR. The first step is to evaluate whether the organization processes or holds the information of any data subject in the European Union. Once that is confirmed, the work begins to ensure compliance.

KPMG's Privacy Methodology establishes the information life cycle as the basis for effective Privacy controls in an organization, aiming to identify and manage the risks associated with personal information from its creation through to disposal.

Compliance Transformation Framework

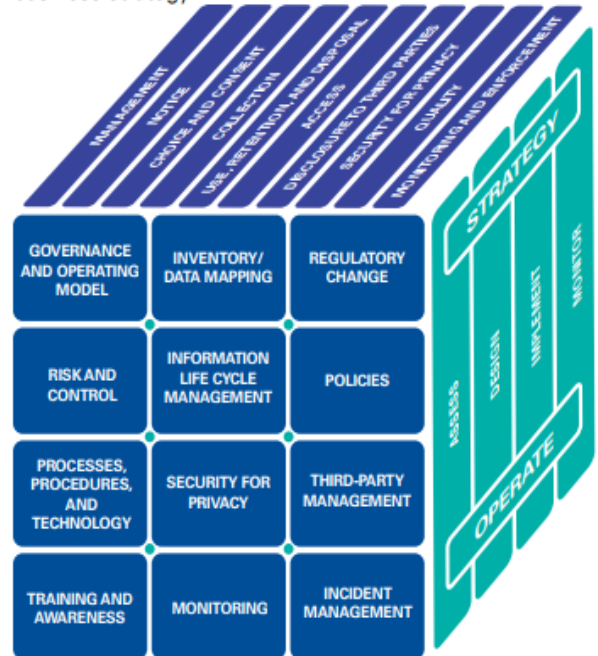
Compliance programs must be assessed and enhanced in response to new privacy regulations, such as GDPR. Key considerations include evaluating the organizational structure to appoint a Data Protection Officer, developing and updating a centralized inventory of privacy obligations and mapping them to policies and procedures, reviewing vendor relationships, completing risks and control assessments, conducting compliance testing, and developing compliance training and reporting requirements.



Privacy Management Framework and Transformation Cube

Our framework had been used successfully to help identify, define, and manage what is required in executing Privacy compliance programs and running day-to-day Privacy operations. Accelerators used in conjunction with the framework include a Privacy law repository, multijurisdictional Privacy controls gap analysis, and Privacy Impact Assessment tool.

To manage their privacy risks, organizations should implement risk-based approaches that are tailored to their individual privacy needs, risk appetite, and future business strategy.



*** - (30)

Benefits of KPMG's Service Offerings for GDPR compliance:

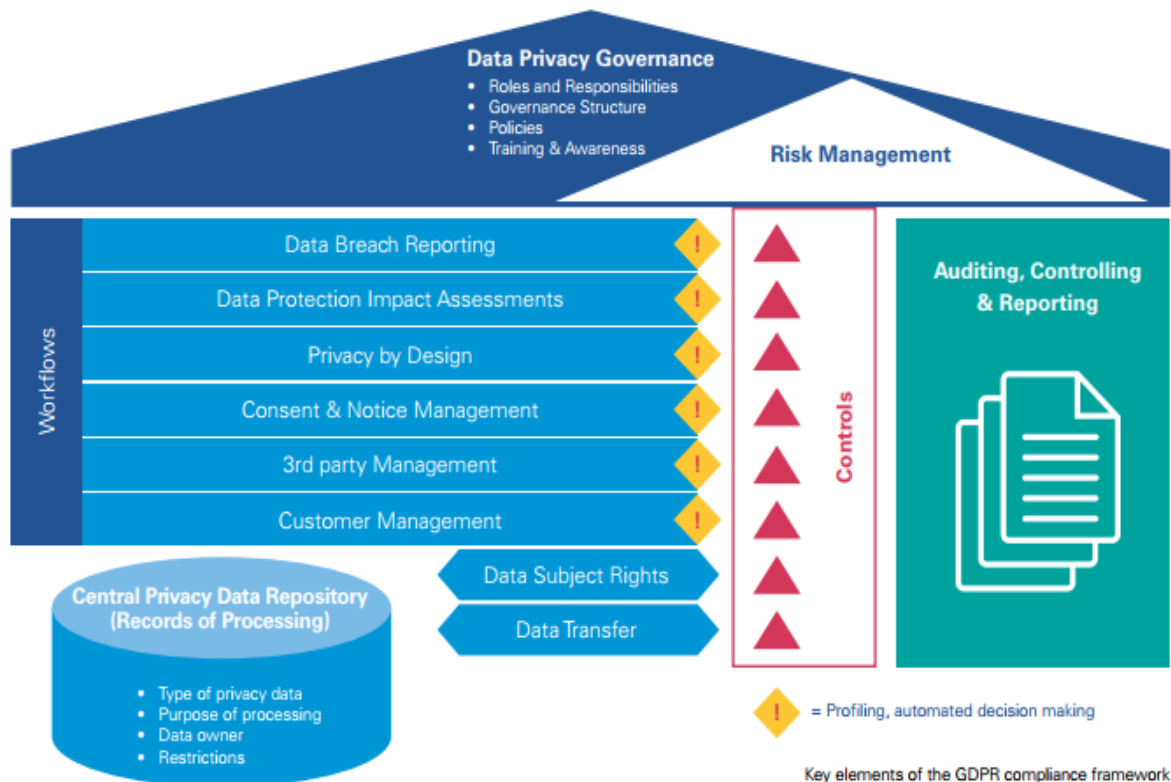
- Greater insight into data stored within unstructured environments and identify hidden risks
- Secure management of critical and confidential personal data
- Policies and procedures to help ensure the protection of the company's crucial assets
- Design and implement proactive monitoring "get clean..stay clean"
- Reduction in data storage costs
- Enables a risk based approach to data governance and data protection by enabling the organization to confidently know what data it has, what's most at-risk, and where it resides
- Identification of sensitive third party data sharing and/or sources



*** - (31)

KPGM technology partners in GDPR implementation are Australian tech firm Nuix and Swiss Software Company OBSERVAR AG that was created in 2004 in a MBO from the KPMG Switzerland. (32, 33)

Last solution is quite innovative.



KPMG, along with its partner OBSERVAR, has developed a technical solution that enables companies to immediately implement GDPR processes and workflows, and therefore gain control over the operational implementation and monitoring of GDPR compliance. KPMG delivers a preconfigured GDPR compliance solution with all relevant content necessary to ensure compliance with the new regulations. The tool further offers customization possibilities and ongoing support.

Within the available enterprise governance risk and compliance (eGRC) functionality, four modules cover the following GDPR items:

- GDPR governance management
- Data ownership management
- GDPR staff training and assessment
- Data protection impact assessment
- Data breach notification
- Privacy by design
- Profiling compliance
- Data minimization management
- Consent management
- Processor and 3rd party management
- Controller management
- Notice management

The key advantages of using OBSERVAR for GDPR

The current situation includes an increasing number of regulations, and companies are struggling to keep the many regulations under control. As such, many firms are seeking a fast and cost-effective solution for GDPR compliance before the regulation becomes effective in May 2018. KPMG can offer exactly this with the help of the OBSERVAR tool.

Minimal implementation effort/costs

KPMG has parameterized OBSERVAR for GDPR implementation, ensuring that the tool provides the required governance structures, templates (e.g. policies), controls and processes. This saves project and implementation costs.

Time to market

The GDPR module with its pre-defined content enables you to achieve GDPR compliance within a very short timeframe.

It covers:

- Governance models
- Roles and responsibilities
- Templates for policies, guidelines, etc.
- Default processes, e.g. breach reporting
- Standard set of controls and reports

Compliance functions available from day one

All work processes and results are immediately available:

- Workflows
- Documentation
- Progress tracking
- Controls
- Reporting
- Auditability
- Customer-specific configuration and parametrization takes only a few working days
- Customers can easily learn how to parametrize the system

Quick start – Fast technical integration

- Technical provisioning from the cloud is possible within one working day. In addition, it is possible to establish an alternative operation platform (internal or outside solution) at any time
- No system integration required, since the system is a web platform
- Easy integration into Active Directory
- OBSERVAR is a web-based platform and therefore does not require any system integration work

Customized operation platforms

As desired by the client, OBSERVAR can be operated in any scenario:

- Microsoft Azure Cloud
- On-site at the client's premises
- At any outsourcing center

GDPR content service

- Receive the latest GDPR updates
- Get your compliance framework updated by KPMG

High security

- For additional security, OBSERVAR can deploy the tool to be used only in https (using our own certificate for cloud installations or the customer's certificate when installed on-site)
- OBSERVAR can also apply an extra security layer by encrypting the texts when inserted in the database, thus preventing an intruder from seeing entered texts and comments in the event of unauthorized access of the database
- The OBSERVAR eGRC solution can be protected through Cloud Access Security Broker solutions
- The underlying database can be encrypted through different mechanisms (TDE, always-encrypted, etc.)

*** - (34)

Pricing

We did not find any references of KPMG GDPR services pricing on open web sources. However, we think they offer the cheapest pricing among top-5 players due to its Observar solution.

Contact People

Mark Thompson
Global Privacy Lead
KPMG International
E: mark.thompson@kpmg.co.uk

Greg Bell
Global Cyber Security Co-leader
KPMG International
E: rgregbell@kpmg.com

Akhilesh Tuteja
Global Cyber Security Co-leader
KPMG International
E: atuteja@kpmg.com

Doron Rotman
KPMG in the US
E: drotman@kpmg.com

Koos Wolters
KPMG in the Netherlands
E: wolters.koos@kpmg.nl

James R. Arnold
Principal
Cyber Security Services
T: 314-740-2626
E: jrarnold@kpmg.com

Roxann Kerner
Alliance Director II
T: 847-867-5368
E: rkerner@kpmg.com

David Shin
Director Advisory
Cyber Security Services
T: 214-840-2373
E: dhshin@kpmg.com

Vincent Maret
KPMG in France
E: vmaret@kpmg.fr

Leandro Augusto Antonio
KPMG in Brazil
E: lantonio@kpmg.com.br

Luca Boselli
KPMG in Italy
E: lboselli@kpmg.it

Jacinta Munro
KPMG Australia
E: jacintamunro@kpmg.com.au

Souella Cumming
KPMG in New Zealand
E: smcumming@kpmg.co.nz

Ilya Shalenkov
KPMG in Russia
E: ishalenkov@kpmg.ru

Amy Matsuo
Principal and National Lead
Regulatory Insights
T: 919-380-1509
E: amatsuo@kpmg.com

Michael Falk
KPMG in Germany
E: mfalk@kpmg.com

Henry Shek
KPMG China
E: henry.shek@kpmg.com

Atsushi Taguchi
KPMG in Japan
E: atsushi.taguchi@jp.kpmg.com

Mayuran Palanisamy
KPMG in India
E: mpalanisamy@kpmg.com

Dani Michaux
KPMG in Malaysia
E: danimichaux@kpmg.com.my

David Remick
Partner and U.S. Lead
Privacy Services Network
T: 404-222-3138
E: jremick@kpmg.com

We want to sum up this section with GDPR solution's ranking. Based on our analysis such ranking of top-5 players is the following:

- 1. EY (no apparent weaknesses)**
- 2. Capgemini (only weak point: US presence)**
- 3. KPGM (due to innovative "budget" solution)**
- 4. PwC (weak technology partner + scope)**
- 5. Deloitte (weak technology partner + mixed reviews)**

Key Takeaways

Key findings of current research:

- On May 25, 2018, the European Union's new data privacy regulations will go into effect
- The new policy, known as General Data Protection Regulation or GDPR marks a wide-reaching and significant shift in the way that organizations must protect personal data
- GDPR compliance is quite costly business (\$1-4 million)
- More than 25% of SMBs and up to 65% large enterprises will use third parties to support their GDPR efforts
- It creates great business opportunity for IT service providers which can offer GDPR solutions
- Large organization are better equipped to handle GDPR
- Over half of US multinationals say GDPR is their top data-protection priority
- However, most businesses overestimate their GDPR readiness
- First five months of 2018 we will see big activity on the market as most organizations will try to be GDPR compliant before deadline
- Up to 80% of their GDPR allocated budgets will be spent during this period
- After analysis of GDPR offerings of top-5 players on the market we think that EY has the strongest proposition followed by Capgemini

- We determined that average time for full GDPR implementation for organizations is 3-6 months
- All companies keep their pricing confidential and state that its level could be determined GDPR readiness or gap assessment
- We think pricing level for GDPR services is more or less on the same level and it depends rather on project time and working hours since final pricing is based on participated partners' hourly rates which are almost identical for all companies
- That is why KPGM innovative GDPR Observar solution could disrupt current price levels
- However, we think it is more applicable for SMB segment

References

1. <https://www.pressebox.com/pressrelease/idc-central-europe-gmbh/IDC-Predicts-GDPR-Will-Create-a-35B-Market-Opportunity-for-Security-and-Storage-Vendors/boxid/763871>
2. <https://www.veritas.com/content/dam/Veritas/docs/reports/gdpr-report-en.pdf>
3. <https://www.esecurityplanet.com/network-security/over-90-percent-of-organizations-see-challenges-in-complying-with-eu-gdpr.html>
4. <https://www.mediapost.com/publications/article/309342/the-price-of-compliance-study-uncovers-gdpr-costs.html>
5. https://www.sas.com/en_gb/news/press-releases/2017/september/gdpr-challenges.html
6. <https://www.pwc.com/us/en/increasing-it-effectiveness/publications/general-data-protection-regulation-gdpr-budgets.html>
7. <https://www.pwc.com/us/en/increasing-it-effectiveness/publications/gdpr-readiness.html>
8. <https://www.accountancylive.com/92-european-businesses-not-ready-gdpr>
9. [http://www.ey.com/Publication/vwLUAssets/ey-gdpr-demanding-new-privacy-rights-and-obligations/\\$FILE/ey-gdpr-demanding-new-privacy-rights-and-obligations.pdf](http://www.ey.com/Publication/vwLUAssets/ey-gdpr-demanding-new-privacy-rights-and-obligations/$FILE/ey-gdpr-demanding-new-privacy-rights-and-obligations.pdf)
10. [http://www.ey.com/Publication/vwLUAssets/EY-Can-compliance-help-you-compete/\\$FILE/EY-Can-compliance-help-you-compete.pdf](http://www.ey.com/Publication/vwLUAssets/EY-Can-compliance-help-you-compete/$FILE/EY-Can-compliance-help-you-compete.pdf)
11. [http://www.ey.com/Publication/vwLUAssets/EY-eu-general-data-protection-regulation-are-you-ready/\\$FILE/EY-eu-general-data-protection-regulation-are-you-ready.pdf](http://www.ey.com/Publication/vwLUAssets/EY-eu-general-data-protection-regulation-are-you-ready/$FILE/EY-eu-general-data-protection-regulation-are-you-ready.pdf)
12. <http://www.ey.com/gl/en/newsroom/news-releases/news-ey-to-help-businesses-comply-with-eu-general-data-protection-regulation-in-collaboration-with-microsoft>
13. [http://www.ey.com/Publication/vwLUAssets/EY-gdpr-microsoft-presentation/\\$FILE/EY-gdpr-microsoft-presentation.pdf](http://www.ey.com/Publication/vwLUAssets/EY-gdpr-microsoft-presentation/$FILE/EY-gdpr-microsoft-presentation.pdf)
14. https://www.pwc.ch/en/publications/2017/gdpr_banking_industry_report_en.pdf
15. <https://www.pwc.com.au/assurance/gdpr.html>
16. <https://www.capgemini.com/wp-content/uploads/2017/09/gdpr-threat-overhead-or-opportunity.pdf>
17. https://www.capgemini.com/wp-content/uploads/2017/07/gdpr-readiness-brochure-web_v1.pdf
18. https://www.capgemini.com/wp-content/uploads/2017/07/how_to_get_ready_for_the_gdpr.pdf
19. https://www.sas.com/en_us/partners/find-a-partner/alliance-partners/capgemini.html
20. <https://www.capgemini.com/2017/02/the-top-10-things-to-know-about-the-gdpr-and-how-capgemini-can-help-yo-0/>
21. <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-gdpr-vision-approach.pdf>
22. <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-gdpr-preparing-for-a-new-era-in-privacy.pdf>
23. <https://bem-symfony-content.s3-eu-west-1.amazonaws.com/business/uploads/file/25/256400/18571592-deloitte-gdpr.pdf>

24. <https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-ranked-1-gartner-in-security-consulting-for-5th-consecutive-year.html>
25. <https://diginomica.com/2017/09/26/deloitte-gets-hacked-shoots-self-face/>
26. <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-gdpr-vision-approach.pdf>
27. <https://www.ataccama.com/news/ataccama-announces-partnership-with-deloitte-for-gdpr-compliance-solutions>
28. <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-gdpr-preparing-for-a-new-era-in-privacy.pdf>
29. <https://www2.deloitte.com/content/dam/Deloitte/hu/Documents/tax/hu-tax-shokokai-seminar-gdpr.pdf>
30. <https://assets.kpmg.com/content/dam/kpmg/us/pdf/2017/10/gdpr-pov.pdf>
31. <https://assets.kpmg.com/content/dam/kpmg/us/pdf/2017/04/kpmg-nuix-gdpr-compliance-and-solutions.pdf>
32. <https://www.nuix.com/fact-sheets/kpmg-and-nuix-alliance-finding-facts-human-generated-data>
33. <http://observar.ch/en/about/>
34. <https://assets.kpmg.com/content/dam/kpmg/ch/pdf/observar-gdpr-solution-en.pdf>