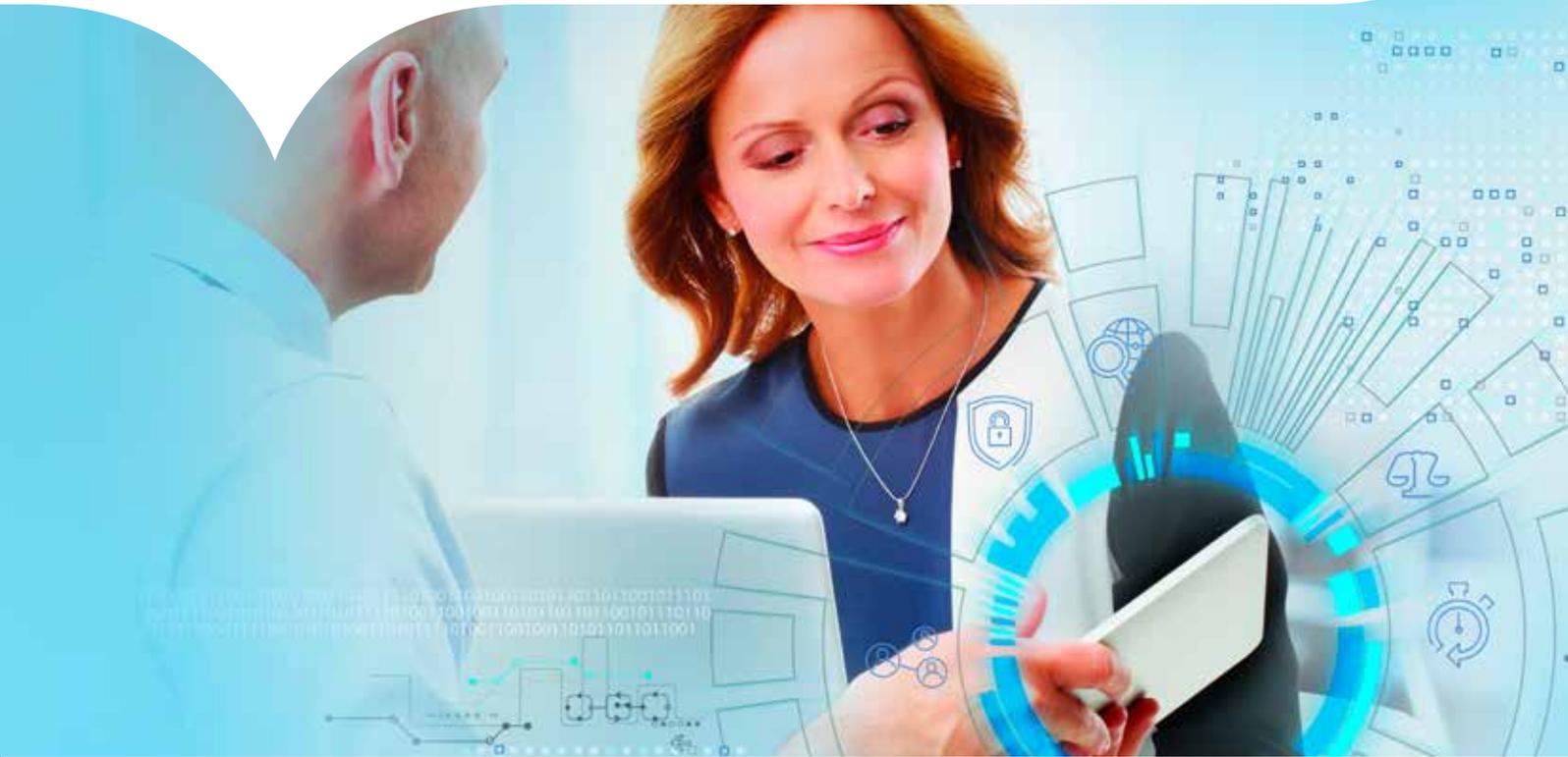


Data protection in light of the GDPR

How to protect your organization's most sensitive data



Why is data protection important?

Your data is one of your most prized assets. Your clients entrust you with this data. In our vision data and its security is critical for your operations, innovation and competitive position. You can be more successful in your respective line of business when you manage to get your data security right. Capgemini and IBM are leading companies to help secure your data and can help you prepare for the GDPR as well.

Monitor and control your data

In recent years there have been increasing attacks from malicious third parties to many organizations' systems. Sometimes these are successful. Often they remain undetected. So called 'super users' are people that can access, change and even delete data from your databases. They can do so knowingly and unknowingly. In order to properly protect your data we believe you need to be able to monitor the activities of those super users and if needed, limit their access. You should also log all of their activities. This way you can be more in control and even have reports ready if auditors request it, or when required for forensic investigations.





The GDPR

The General Data Protection Regulation (GDPR) will be enforced on May 25 2018. GDPR is an EU-wide framework for the protection of personal data of EU citizens. GDPR is directly applicable to all organizations that deal with personal data of EU citizens. Organizations will be held more accountable for their data collection and use than ever before. Failing to comply with the GDPR can potentially lead to a fine of up to 4 percent of the worldwide turnover or 20 million euro.

The purpose of this whitepaper is to explain possible implications of the GDPR and how this legislation impacts the way your organization protects and monitors its data. Capgemini and IBM will present a combined set of offerings of products, services and technological solutions that can help you to prepare for the GDPR and protect your data. First, we will provide our view as to why the GDPR is important to your organization. Second, we will describe several fictional organizations and their degree of readiness. Third, we will explain our portfolio and how this can help your organization as you get ready for the GDPR.

IBM and Capgemini are partnering to help you as you get ready for the GDPR and protect your most prized data assets. Capgemini knows how to bridge business issues with technology solutions. We believe that IBM has the best understanding of data.

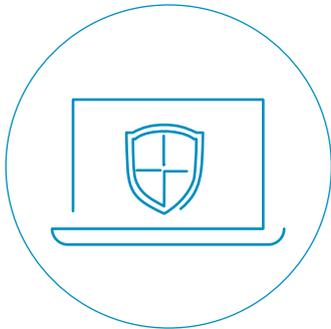
What is the GDPR and why is it important for your organization?

The GDPR is an EU Regulation related to the protection of personal data and free movement of such data. The GDPR requires a very systematic and comprehensive management of data security. It requires data protection management, reporting and accountability mechanisms, including a requirement to notify data breaches, map data flows and conduct data protection impact assessments. The GDPR provides enhanced rights for individuals and increased scrutiny by regulators. Non-compliance may lead to substantial fines.

When the GDPR comes into force, many organizations will be required to have a Data Protection Officer (DPO) and a fundamental understanding of the processes and the classification of the data. A data subject's consent to the use of his/her personal data should be given by a clear affirmative act. Organizations will be required to notify the authorities and to communicate the data breaches to data subjects. Other obligations, such as data protection impact assessments will come into force, too. Violation of the GDPR may lead up to fines equaling 4 percent of the total worldwide annual turnover or 20 million euro – whichever is higher.

Are you ready for the GDPR and to better protect your data?

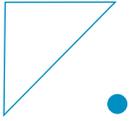
IBM and Capgemini work with organizations from all industries across the globe. Together, we have a deep understanding of the GDPR, associated business challenges and technology solutions. Below are three hypothetical examples where we illustrate how IBM's and Capgemini's offerings can jointly assist you as you prepare for the GDPR. The challenges described in these organizations reflect the preparatory work we see in practice.



Example 1 - Globally operating manufacturing company

A multinational company has outsourced a large part of its IT to IT vendors, partly offshore. It has a large application landscape with many underlying databases. The company's business model is both business-to-business and business-to-consumer. The company holds personal data as well as confidential data and knows the location and nature of this data. Multiple teams have access to the systems and the data for maintenance and support purposes. Recently one of the organizations critical systems experienced significant down time because a database administrator (DBA) accidentally altered critical data. Customers were unable to access the customer portal which led to delays in service delivery and complaints. The customer asked Capgemini to identify the problem, critical systems, system interfaces, develop solution architecture for using IBM Guardium. In doing so the company would have the ability to monitor and control the activities of its 'super users' with respect to its most sensitive data. Capgemini implemented several operational changes related to access procedures and audit trails. Also, parts of the IBM Guardium technology solution were implemented. This involved data activity monitoring and encryption of sensitive structured data. This way the company has better control over its confidential data and is better positioned to detect unintentional alterations to the data or unauthorized access.





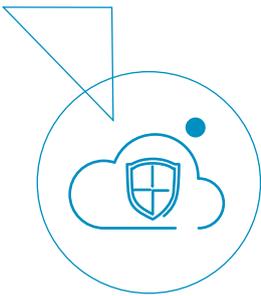
Example 2 - European online retailer

An EU based online retailer provides business-to-consumer products and services. The company holds large amounts of personal data of a large number EU citizens. This includes for example name and billing address and credit card details. It has stored the data in databases and in unstructured locations such as shared folders. The company has no insight into the type of data it holds and does not know if they are legally permitted to store that data. It is unclear who is responsible for the data and no data protection officer (DPO) has been appointed. The customer asked Capgemini to support their effort to be compliant with the GDPR. Capgemini proposed to conduct an assessment and road map to provide insight into where the company stands and provide an actionable strategy for helping the retailer solve their outstanding issues with regard to the GDPR. Capgemini first mapped which type of personal data exists and where it is located and what are the associated risks. Together with the client Capgemini proposed to implement procedures to store, delete and give better control over its data. This enabled the company to better respond to a customer request for accession, deletion or portability of his/her data. Capgemini and IBM proposed Guardium as a solution to give the company insight into how data is being accessed, alert on anomalous activity when detected, and automate the reporting process, which the retailer could use as part of their regulation compliance protocols.



Example 3 - Medium sized public organization

A public organization provides unemployment benefits to its citizens. To do that it processes significant amounts of personal data of eligible national residents. The organization has experienced a recent data breach where vulnerability was exploited in one of its databases containing personal data. Data was taken and published online. This caused public outcry and significant harm to the reputation of the organization. The public organization took the events as an opportunity to reassess their readiness in terms of regulatory compliance (GDPR). It also wanted to take some crucial general data protection measures. It requested Capgemini to conduct a GDPR readiness assessment and road map. This provided the organization with insight and an actionable strategy to help them address their outstanding GDPR related issues. Capgemini proposed several quick wins in terms of technology such as a vulnerability assessment to scan the organization's systems for technological vulnerabilities and design flaws. It also proposed steps to mitigate these risks.





How can we help?

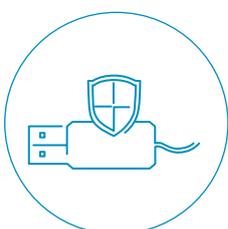
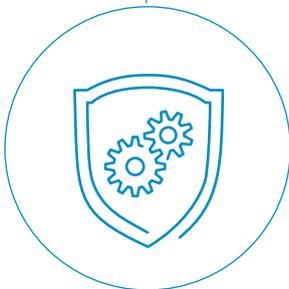
IBM and Capgemini are partnering to help you as you get ready for the GDPR and protect your data. We have designed a combined set of offerings that may fit into your needs to prepare for the new Regulation, whether you are ready or still have a long way to go. Our portfolio considers what we believe to be the most important topics for executives regarding data protection and security. Our portfolio consists of four categories:

- GDPR readiness assessment
- Data security road map
- Business or privacy impact assessment
- Technology solution: IBM Guardium

GDPR assessment

Capgemini proposes a two-week assessment which provides an analysis and recommendations on planning, governance, process, culture, data and technology. The assessment is performed by a team of three specialists who collect and analyze the available materials on the aforementioned categories, interview key persons responsible for these areas in the light of the GDPR and check relevant databases for materials related to data protection. The result of the assessment is a list of categorized findings, conclusions and actionable recommendations for you as you prepare for the GDPR. This is the foundation to get ready for GDPR. The assessment may be the first step towards implementation of other categories, such as planning, governance, process, data and technology. In particular, the following areas will be assessed:

- Individual Rights: review of and assess your internal processes.
- Data Breach Notification requirements: review and assess your organization's readiness regarding data breach notification to Supervisory Authorities and individuals.
- Record Keeping: review and assess your organization's current databases, records, and archives to see what is in place and what is potentially missing.
- Data Protection Officer ("DPO"): assess the need for your organization to have a DPO and review the current position of a DPO (if any) to evaluate what organizational changes are needed.
- Consent and Notice: review customer-facing materials to help you comply with new consent and transparency requirements (and if applicable, in particular with respect to data analytics, profiling, free services and digital offerings to children). Third Party Agreements: review and update agreements and templates with your organization's data processors (suppliers, partners, etc.).





Data security road map

Capgemini proposes to include into your strategic plan for the GDPR a set of defined action items that employ the use of technology and are designed to raise the quality and level of personal data protection within your organization. The development of the plan will involve the stakeholders of your organization and result in a realistic, supported, and actionable plan. Capgemini will facilitate plan development and use its experience of strategic plan development, GDPR readiness capabilities and gained insight into your business and technology solutions. A data security road map can be developed in two to four weeks – or in a two-day concentrated workshop with all stakeholders.

Business or privacy impact assessment (B/PIA)

Capgemini proposes 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, potential risks and measures is generated. The tool provides for each role a dashboard with gaps, risks scores and possible mitigating measures which are categorized. Subsequently a consolidated internal (board) and external report can be generated. The results provide the starting point for an improvement plan for the Data Protection Officer.



GDPR technology solutions

Capgemini proposes the project management, and IBM the technical implementation of Guardium which is a comprehensive data protection platform designed to safeguard critical data, from databases to big data, cloud, file systems and more. Its benefits:

- Five steps to protect critical data: (1) define, (2) discover, (3) baseline, (4) protect and (5) monitor.
- Helps with data discovery, classification, vulnerability assessment, and entitlement reporting.
- Provide monitoring, threat detection analytics and protection for sensitive data in databases and file systems.
- Dynamic blocking and masking of sensitive data, trigger alerts for unauthorized data access, and quarantine.
- Helps to automate reporting, monitoring of controls and support auditing.



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 helps create a path to readiness for GDPR, as well as improved risk mitigation. Additionally, readiness for GDPR can improve your overall data management, which in turn can help protect your data assets.

Please contact us for more information

Contact details:

Kim Boermans

Capgemini
kim.boermans@capgemini.com

Brian Flasck

IBM
brian.flasck@uk.ibm.com

Capgemini Nederland B.V.

P.O. Box 2575, 3500 GN Utrecht
Tel. + 31 30 689 00 00
www.nl.capgemini.com



About Capgemini Sogeti and IBM

With more than 190,000 people, Capgemini is present in over 40 countries and celebrates its 50th Anniversary year in 2017. A global leader in consulting, technology and outsourcing services, the Group reported 2016 global revenues of EUR 12.5 billion.

Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Sogeti is a leading provider of technology and software testing, specializing in Application, Infrastructure and Engineering Services. Sogeti offers cutting-edge solutions around Testing, Business Intelligence & Analytics, Mobile, Cloud and Cybersecurity, combining world class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 25,000 professionals in 19 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the the Paris Stock Exchange.

IBM is a global cloud platform and cognitive solutions company, which has continually evolved over the past century to remain at the forefront of technological innovation, operating in over 60 countries.

Learn more about us at

www.nl.capgemini.com and www.sogeti.nl
www.ibm.com

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