A guide to the

EU General Data Protection Regulation

and the application of

RegTech

How to use RegTech to comply with GDPR and other Regulations *and* create additional value

Planet Compliance

Contents

Foreword

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018. It is one of the most challenging regulatory initiatives and is going to transform the rules governing data protection and privacy in the European Union and beyond.

Like GDPR many other new regulations have increased the pressure on financial institutions where compliance has become a burden for the business in terms of costs and resources that cannot be faced with traditional methods anymore.

Regulatory Technology (RegTech) is often cited as the solution that empowers firms from all industries to deal with these rules. Its true value in our opinion goes way beyond the view of it as a stopgap solution. RegTech is an opportunity for organisations to create additional value ***and*** regulatory compliance. It is sometimes difficult to understand this when we talk about RegTech in abstract terms, so we decided to partner up with eccenca, a software and solutions company, to explain in a use case scenario in concrete terms the real significance of RegTech.

The book will provide an introduction to RegTech and its game changing strategies and technologies. It also offers a detailed introduction to the GDPR and the challenges it brings. Lastly, using eccenca's solution, we describe how this solution can be used to achieve regulatory compliance while creating insights into your company you never had before.

We hope you find this guide useful and look forward to welcome you at www.planetcompliance.com, the leading platform for insights and analysis
Services Regulation and Innovation.

PlanetCompliance

Introduction

Regulatory Technology aka RegTech is revolutionizing how we deal with regulation. The Financial Conduct Authority of the UK defines RegTech as a sub-set of FinTech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities. In reality, RegTech is not limited to financial services alone but rather is applicable in any regulated industry. That's one of the reasons that makes it so attractive. It has already had a significant impact in financial services though as it helps to overcome the old ways of spread sheets in an industry that has come under immense regulatory pressure with a massive amount of new rules coming into force or on the table. Clever start-ups as well as more established players use innovative technology like Smart Data Analytics, Artifical Intelligence or Blockchain to help banks comply with their regulatory obligations. It covers a wide range of aspects and one of the main areas for disruption through RegTech is the communication between different systems, be it internally between existing ones or with new systems, or between different institutions. Most financial institutions work with legacy systems that have been tweaked and amended over several years to become individual configurations that struggle to talk to other systems. A senior IT colleague ones told me that overcome these issues would be like a heart transplant surgery, where the old one basically needs to be removed first before the new one can take its place only that it would be like replacing several hearts at the same time.

However, new regulation and notably MiFID II has brought challenges, in particular with respect to reporting requirements and the management of data for firms and service providers that has made significant investments in technology inevitable.

Another key field of application lies in the management and analysis of the huge amount of data financial institutions hold. Compliance Monitoring for the purposes of fraud detection or suspicious activity from a Market Abuse, AML or CFT perspective are areas made for disruption by new entrants and old ones alike if they can come up with a better solution.

KYC and Due Diligence in general are also very popular with RegTech start-ups. Financial institutions have long been waiting for solutions that allow them to access and manage their data more efficiently and streamline the current setup while saving money and resources on what is a now costly and time intensive process.

However, despite a lot of attention, which RegTech has received particular in the last twelve months, several obstacles have to be overcome. For instance, in order to further advance RegTech, it will be important to create further awareness and better understanding among the decision makers in financial institutions of the benefits it could bring to the industry.

Chapter 1: The Real Opportunity of RegTech

Whenever talk turns to regulatory initiatives and how RegTech can solve these challenges, it seems that we do not appreciate the real opportunity of RegTech: Transparency about your internal policies, processes and the related datascape. Yes, it may appear to be the only way to get to grips with the constant regulatory change and the enormous obligations that come with regulations like MiFID II or GDPR. But looking at how RegTech works in practice, we discover that the true value goes way beyond the solution of specific problems.

RegTech now and then

The last year has put RegTech in the spotlight and created a kind of hype about it, but many believe that 2018 could be the year we find ourselves at crossroads. With a year full of regulator challenges in the form of MiFID II, GDPR, PSD 2 and many other initiatives becoming applicable, can RegTech live up to its promise? We at PlanetCompliance certainly believe so. Not only because traditional methods and spreadsheets won't be able to deal with the immense demand for information that authorities ask for. It needs new ways to address these challenges effectively and this is what RegTech is first and foremost supposed to do. While most RegTech solutions might tackle a specific problem though, the real value goes beyond this as they are able to create an original and efficient approach. Effectively, they offer application in other uses cases that can present new opportunities and increase their attractiveness many times over.

Take, for example, compliance with the General Data Protection Regulation (GDPR). Designed to harmonize data privacy laws across Europe, it presents companies with immense challenges to ensure compliance with its requirements. However, addressing only the requirements of this particular act, means ignoring the potential to deal with future regulations in a more efficient and cost effective way.

At the bottom of the problem

Why? Well, at the bottom of most of the challenges that financial institutions face is data, or to be more precise transparency about our datascapes and the quality of the information held by organisations. Institutions hold incredible amounts of data, but this data comes from numerous sources in multiple applications, everything encoded so that only the respective source application can decode and interpret the information. That's what makes the reuse of data so difficult and leads as a result with regard to the requirements introduced by the GDPR to a high risk of non-compliance as well.

This is the point where RegTechs like eccenca can help though: actually, most information kept in the code of applications can be described as data, and, by doing so, can be removed from the specific context of the source program, analysed and linked at data level to create single clouds of metadata, which in turn then can be used again. The trick is to make sure that data isn't simply copied over from one application to

another one and duplicated. In this way, the data is reusable for other purposes. This process adds even more value when data is shared with external sources such as trade bodies and industry associations but on a bilateral level, too, since often data standards cover only a fraction of data usage, for instance, the communication with exchanges for reporting purposes.

The RegTech Opportunity

In most cases RegTech does not only present a solution for one particular problem, but consists of value that goes well beyond the application to a single case. And GDPR is an excellent example to show how: the problem with complying with data protection regulation is that data subjects are scattered across dozens, if not hundreds of systems in an enterprise. A client of a bank could be registered for one product in one system and for another product in another system and so on. Regularly, financial institutions hold information in many places about the same client, but have no idea about what and where. The eccenca solution collects metadata from the various systems, consolidates the information and can provide an internal map of personal data processing, always up-to-date as basis to answer subject access requests about data usages in accordance with GDPR, e.g. which information does the company hold about the client, where, why, on which legal grounds, how and when approved, and for which purpose. In this manner the solution creates exactly the kind of absolute data transparency required by the regulation, without duplicating the data itself.

If you have to go through this not small exercise, it stands to reason that you would also use the results for other purposes. On the condition that permission has been given, these insights empower a firm to gain a better understanding of their clients and, as a consequence, discover and explore business opportunities, or address other regulatory challenges. It is necessary though to appreciate and embrace these opportunities. For a firm and its culture, it requires a certain mind-set and openness towards innovation rather than the intention to find a quick fix, as it doesn't do RegTech justice. After all, while it is an excellent way of dealing with the constant regulatory change, it is foremost an opportunity to gain a competitive advantage and see your organisation like you've never seen in before.

Chapter 2: GDPR = Challenges and a Unique Chance

As the first chapter served to explain that for RegTech to fulfil its entire potential, it needs to be something more than an instrument used to simply address isolated regulatory requirements, it is now time to dive into the practical example: GDPR. A very demanding new set of rules to say the least, with the right solution you can achieve comprehensible and trustworthy evidence; the solution should bring transparency on a firm's compliance status; it should also create actionable insights in a manner that is easy to access and easy to understand. Only then RegTech truly lives up to expectations and makes GDPR compliance a competitive advantage.

How do you achieve this though? Well, it's probably best to use an example of a RegTech solution, the regulatory challenge, and how the solution addresses the requirements set by the regulation as well as creates additional value that goes beyond the initial objective and improves a firm's framework several times over.

So, let's begin with the details of the regulatory challenge, the GDPR.

The GDPR principles

GDPR: Data Protection re-invented

Protection of personal data is at the centre of the regulation. This principle is one of the fundamental rights set out in the Charter of Fundamental Rights of the European Union. The EU felt that it is one of those rights that cannot be stressed enough as you can tell from the regulation's preamble:

> *"The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."*

The European lawmakers also felt that the existing framework did not provide this level of protection, so they set out to produce new rules and after four years of work the regulation came into force on 24 May 2016. The GDPR will apply from 25 May 2018 and set a new standard for the protection of personal data. With the GDPR the European Commission aims to harmonize and strengthen data protection for all individuals within the European Union. A formal organizational framework will be setup in all member states to enforce the adoption of the GDPR. It is not just to secure or to store data and information, but to care for the data and information of individuals. Companies will have to observe the regulatory environment, the technical environment, and the process-related environment to really manage data. Last but not least, companies will have to react to new upcoming demands by those affected.

It is safe to say that the GDPR is one of the most challenging regulatory initiatives of all times as it requires extensive data management, an entire re-evaluation of risk positions, an increase to the maturity of procedures, systems have to be compliant by default and design, and one has to prove compliance with GDPR. Because if that is not

the case the consequences will be severe as we are going to see in detail further down below.

The Basics

All systems and procedures, which process personal data automatically, are in the focus of the GDPR. The definition of personal data in various contexts can differ significantly and if in doubt, it is advisable to rather assume data to be personal than not. As some data are obviously personal, others may only appear to be so at a second glance. For example, asset information like MAC or IMEI addresses are defined to be personal data, too. The situation becomes even more complicated when considering that data may be handled differently in different contexts.

The GDPR also adds a whole new dimension in terms of territorial application. It will affect any company doing business in the EU and is applicable to all personal data of individuals, which are citizens or residents of the European Union regardless where the controller or processor is based in. Therefore, it is important to acknowledge that persons from outside the EU may belong to the GDPR regime as well.

The GDPR also aims to protect data throughout its entire life cycle: from its collection, to processing, storage, updates, transferals, archive, all the way to its erasure. All operations on data are affected by the GDPR.

The essential principles guiding the regulation are:

- Lawfulness, Fairness and Transparency
- Purpose limitation
- Limited storage periods
- Data quality
- Data minimization
- Accountability
- Information security
- Data protection by design and by default
- Legal basis for processing
- Requirements for onward transfer

To be compliant with the GDPR, companies have to be aware that they must have high transparency where personal data is stored, which relations exist among the various data storages, by whom it is processed, and who is using it. On that matter companies have to provide evidence. Data flow, data storage, and data quality are essential to all these areas.

Strict Enforcement

One of the key findings during the law-making process was that the assertion of data protection and its application had been relatively weak in the past. With this regulation

accountabilities are enforced by penalties for companies as well as for the acting people, namely top management and the Data Protection Officer. The stick that the EU is going to use against offenders has two ends: substantial administrative fines and an extended basis for claims.

Administrative Fines

The probability of administrative fines has drastically increased with the GDPR. They can rise up to 20 million Euros or up to 4% of the worldwide annual turnover of the offender. However the GDPR explicitly states that one can lower the fines if efforts around data protection are comprehensibly evident, constructive, and proactive. Data subjects may also raise a claim for non-monetary loss and involve a syndicate to file an action on their behalf. Penalties out of those claims are not already covered by administrative fines and will come on top of the financial risk. The burden of proof of compliance with the GDPR lies entirely upon the offending data controller against whom a claim has been filed. It is up to the data controller to build a proper contractual framework with other service providers which process the data to make them liable for any state of noncompliance.

Extended basis for claims

Along with the reverse burden of proof that now lies with the provider, also the applicability of claims is widened. Each controller and processor can be made liable in case of damages. The range of this accountability covers the entire damage. If multiple processors are involved in a claim, the one who fully compensated for the damage may claim the other processors for compensation. Data controllers as well as data processors have to be prepared to be able to follow the GDPR.

Conclusion

If there had been any doubts about the width and impact of the GDPR you now know better. However, so far we only have scratched the surface. In the next chapter we will delve into the details of the new rules. Maybe more importantly though, we will also show you how a challenging regulatory initiative can tackled to achieve compliance with a firm's obligations ***and*** achieve cost savings as well as a competitive advantage with the right solution.

Chapter 3: GDPR and Data Subject Rights

Following our general overview of the GDPR, we will now look at Data Subject Rights – the challenges they bring and how to deal with them.

Data Subject Rights – The Challenge

The GDPR strengthens the rights of individuals to be able to fully control their personal data. Those rights will change the daily operation of data and demands also a proper organizational setup and in most cases organizational changes.

As a consequence, about 10 core use cases can be identified that define obligations of an organization towards data subjects:

(Please note that there are more duties not directly related to relationships with data subjects, focusing on the duties of data controllers vs. data processors and the transfer of personal data to third countries).

Supply information when collecting personal data

The controller has to provide information to individuals relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. Providing information in the form of privacy policy that are excessively lengthy or difficult to understand is not permitted.

The scope of information that needs to be provided is outlined in articles 13 and 14 of the GDPR, but the controller might be required to provide additional information if the particular situation makes it necessary.

Provide access to personal data on request

In accordance with Article 15 GDPR, individuals have the right of access to personal data. This means that the controller has to provide a copy of the personal data undergoing processing, which needs to be provided free of charge. However, the controller can charge a reasonable, administrative-cost fee, in case of repetitive requests, manifestly unfounded or excessive requests or where additional copies are requested. This right is based on the argument that individuals are aware of and can verify the lawfulness of the processing.

Manage consent for processing purposes if no other legal basis applies

The processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law and all data processing activities require a lawful basis, which can come in the form of an individual's consent. If the processing of personal data is based on the data subject's consent, the controller has to be able to demonstrate that the data subject has given consent to the processing operation. The data subject shall have the right to withdraw his or her consent at any time. The

withdrawal of consent should not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof and it has to as easy to withdraw as to give consent.

Manage rectification of personal data on request

A data subject has the right to demand the rectification of inaccurate personal data concerning him or her from the controller. In specific cases, depending on the purposes of the processing, individuals can ask to have incomplete personal data completed, or to add a supplementary statement.

Manage objection or restriction of processing of personal data on request

While the data subject does not have a general right to object to the processing, there are several situation where a specific right to object exist such as where the processing is carried out for specific purposes, or where the right to object is justified on a particular basis. These cases include where the processing is for direct marketing purposes; where the processing is for scientific or historical but which requires grounds relating to the data subject's particular situation unless the processing is necessary for the performance of a task carried out for reasons of public interest; and where the processing is based either on legitimate interest grounds (for example, in a case of 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) or it 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.

The controller must then cease processing of the personal data unless an exemption applies, i.e. the controller can demonstrate compelling legitimate grounds which override the interests of the data subject; or where the processing is for the establishment, exercise or defense of legal claims.

Manage erasure of personal data on request (right to be forgotten)

The right to erasure or 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. Again, this right does not constitute a general claim, but targets specific circumstances, which are defined in Article 17 GDPR:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- The individual withdraws consent.
- The individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed.
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Notify third parties of those rectification, restriction or erasure

To address the importance of a data subject's rights, for instance, in an online environment, the controller is obliged to inform other controllers who are processing the data that the data subject has requested erasure of those data, where the controller has made personal data public, and where it is obliged to erase the data. The controller has to take reasonable steps and account must be taken of available technology and the cost of implementation. The controller must notify any one to whom it has disclosed such data, if the controller has to erase personal data unless this would be impossible or involve disproportionate effort.

Give back personal data on request and allow transfer to other data controllers (data portability)

Where the processing is based on consent or carried out by automated means, individuals have the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. This right to data portability aims to enable the data subject to obtain and reuse their personal data for their own purposes across different services.

Do not base decisions about data subjects solely on automated means

An individual has the right not to be subject to a decision based solely on automated processing, including profiling, if the decisions produce legal effects or similarly significantly affects the data subject. The GDPR gives the example of an online credit application or e-recruiting practices without any human intervention. The regulation also outlines that such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. Exceptions to the rule are possible though in case where the decision is necessary for entering into, or to perform, a contract between the data subject and the controller; the significant automated processing is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or is based on the data subject's explicit consent.

Communicate personal data breaches (specific conditions apply)

Data controllers have to communicate a personal data breach to the data subject without undue delay if the breach is likely to result in a high risk to the rights and freedoms of natural person. The notification needs to be in clear and plain language and explain the nature of the personal data breach and contain at least a minimum of information such as the name and contact details of the data protection officer or

other contact point where more information can be obtained; describe the likely consequences of the personal data breach; and explain the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Data Subject Rights – The Solution

Now that we have the defined the obligations and challenges of the GDPR with regard to the data subject rights, we can think about how to address them. eccenca is a RegTech company whose next generation data management solutions are driving automation and rationalization for metadata management, data integration, analytics and data driven processes.

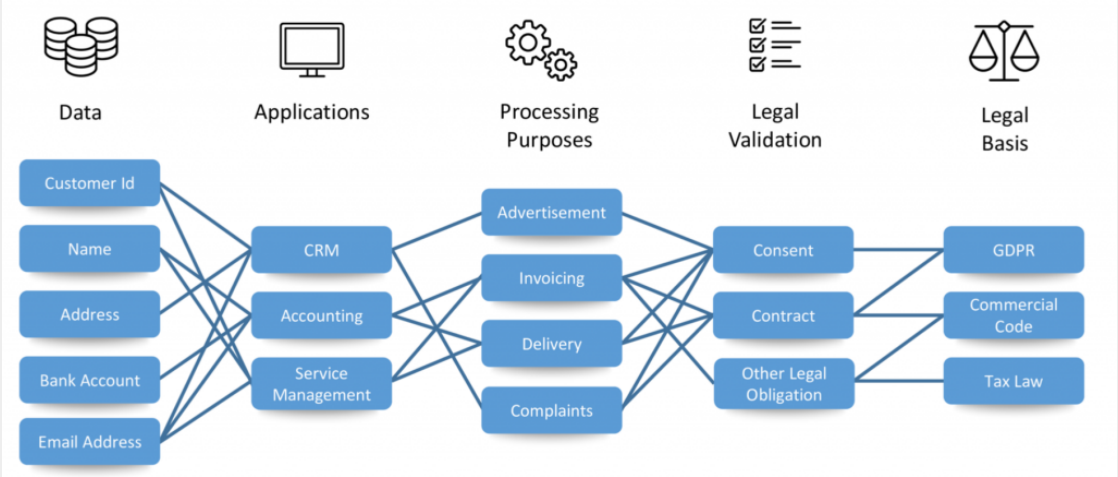
From a purely technical perspective the eccenca Corporate Memory solution combined with the eccenca GDPR Solution package addresses the data protection function by delivering a granular map of the complete personal data landscape. This map can then be used to identify all personal data of a data subject to fulfil subject access requests (SAR).

The system can answer relevant question for each data subject ID: which personal data items are there, who is the data controller, who is the data processor of those, in which system is each processed, what is the attribute name, what is the processing purpose and the legal basis (e.g. consent). Everything required to handle SAR and to provide full transparency to the data protection officer, without exposing any actual personal data. It does NOT store the values of the personal data, those are only managed in the respective systems.

The complex grid of dependences

The underlying technology stack is built on RDF graph technology, which can quickly be adapted to evolving requirements. The metadata described is collected from the various source systems either via a standard API provided for this use case or as fall back via an Excel roundtrip.

There is a user interface geared towards the data protection function to explore and search this map and there are APIs and endpoints to access it via third party tools for analytics and reporting.



The complex grid of dependences

Architecture of the eccenca Corporate Memory – GDPR Solution Package

To internally manage subject access requests the eccenca GDPR solution provides integration with a standard tracking tool (JIRA) to route incoming requests within the organisation.

By doing so, a firm achieves a competitive advantage, increased reliability, and reputation. It also results in simplified data management operations as well as the ability to process across company borders and get full transparency on data storage.

This in turn means that data processing costs are lowered through simple and fast identification of related data. Operational risk costs are reduced by full transparency and causes a higher turnover based on competitive advantage in personal data sensitive businesses.

The picture is similar from the data subject interaction perspective. The data protection function of the GDPR requires firms to comply in terms of their duty to supply information, consent management, and the right to object. The eccenca Corporate Memory tags specific data i.r.o. 'consent', 'objection', or 'legitimate interest'. It sets rules to identify personal data of children for special treatment in terms of children's consent. The solution relates 'consent', 'objection' and 'legitimate interest' to respective systems, procedures / processes, and purposes. Again, relations among semantic identical data are built without causing redundancy. The set rules identify data to be of the same kind and generate a report with all relevant information supply.

The value added is both in compliance and financial terms. From a compliance perspective it delivers proof of GDPR compliance and creates a competitive advantage

through increased reliability, and reputation. It builds trust and transparency to the data subject. The financial value comes in terms faster and cheaper and more reliable processing of SARs, of lower administrative fines in case of noncompliance, lower data processing costs, no redundant information and higher turnover based on competitive advantage in personal data sensitive businesses.

Conclusion

The example of the data subject rights as established by the GDPR clearly shows how a challenging regulatory initiative can be tackled to achieve compliance with a firm's obligations and achieve cost savings as well as a competitive advantage with the right solution. This is not the end of our guide on the GDPR and the advantages of RegTech. In the next chapter, we will look at additional obligations of organisations as set out by the GDPR and show how regulated institutions can benefit further from using the right RegTech solution.

Chapter 4: GDPR and Organizations' Obligations

It is paramount to understand the data subject rights as defined by the new rules. However, it is equally important to get a good grip on the obligations for organizations. We will therefore in this final chapter tell you about the challenges but also explain the opportunities for an institution that come with obligations for organizations under GDPR.

Organizations' obligation – The challenge

Software may not be the answer to all questions, but it will help organizations to follow their obligations. It is obvious that in times of mass data processing an efficient management of the requirements cannot be met without the support by information technology.

Proof of Compliance

Organizations actively have to prove compliance with GDPR. In that they have to demonstrate their ability to manage data protection and have to show that they can fulfil data subjects' rights as a standard operational task.

Processes have to be implemented whose effectiveness is comprehensibly verified. Data management and good data governance will become a core capability to every company. There is a strong relationship among those compliance frameworks like data protection and information security (and IT security).

Tasks of the Data Protection Officer

The Data Protection Officer (DPO) no longer has only the duty to provide advice on matters of data protection, but must now actively monitor compliance with the GDPR and related rules and regulation. To underline the magnitude of the task, consider that not just the regulation itself is the basis for these duties but other acts as well such as the work of the Article 29 Working Party, which has provided a number of documents and guidelines with quasi-binding effect. Thus, companies have to build structures, which allow the DPO to fulfil his/her now widened duties.

The GDPR specifies a minimal set of duties for the DPO:

- Information and consultancy
- Supervision of company's compliance to GDPR
- Supervision of data protection strategies
- Assessment of data protection consequences
- Cooperation with supervisory authorities
- Risk assessment

Data governance Compliance with GDPR comes along with the requirement of designated responsibilities, functions and allocated budget for data protection. Hence organizations are asked to implement a wide range of measures to comply with the GDPR. Some of those are:

- Data protection by design and default
- Protection impact analysis
- Regular audits and assessments
- Data Protection Officer
- Record of processing activities
- Training and awareness program

Breach Notification

If a breach of personal data has been discovered companies have to notify the authorities without undue delay, latest within 72 hours. If those data are classified as 'high risk' also the data subject has to be notified.

It is obvious that companies should have the right procedures at hand to detect, report and investigate data breaches. This might be a good idea for any sensitive data. In case companies fail to report such data breaches they will face significant administrative fines as well as fines for the damage caused.

(Joint) Accountability

Companies have to prove compliance with the GDPR. This goes beyond Technical and Organizational Measures. Obligatory documentation requirements apply to all procedures dealing with personal data independent from an external access. It is highly probable that additional documentation requirements will be imposed.

It is no longer an adequate data management style to 'store and to forget as long as it is secure.' Companies have to take care of personal data. As soon as data are no longer necessary, delete them — permanently. If the environment changes take care that data are treated in compliance with GDPR. Environment in this context might mean a change of processes, data themselves, regulatory requirements, or even a change in semantic meaning.

GDPR only differentiates between processors and joint controllers. Therefore, the outsourcing of functions seems to be still possible but all parties are made accountable in case of a compliance breach. The data controller as the first service provider to the data subject especially is accountable.

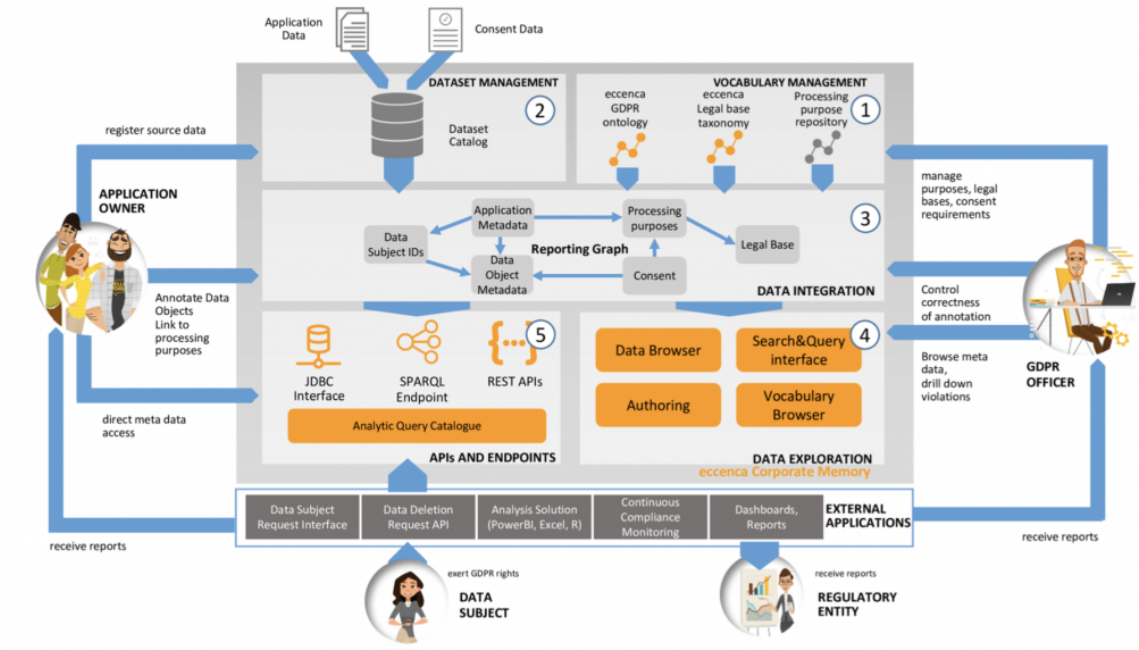
Organizations' obligation – The solution

So much for the challenges, but how should you tackle them? As outlined already before, we believe it is important to address this to achieve a) compliance with the regulatory requirements, but also b) create additional value. eccenca's solution based on its Corporate Memory platform, for instance, supports the aspects in terms organizations' obligation by providing a full map of granular metadata per data subject. This map can be browsed and searched from any perspective to help resolving the new tasks that organizations face.

The map includes the links and pointers to the systems that actually manage the data and show how things are connected, what they are used for (purposes), which are the underlying legal bases and who is data controller and data processor. Understanding the personal data landscape within a company's data processing fabric is key to demonstrate the capabilities requested.

The value added through this approach comes in many forms: it builds trust and transparency to the supervisory authorities. It creates transparency on the data protection risk situation and can serve as a nucleus to improved data governance beyond personal data. Firms achieve higher ability to manage data protection and the response time to audit requests is easier to manage.

In financial terms, the value added comes in the form of faster, cheaper and more reliable processing of SARs lower data processing costs, lower costs of risk.



Architecture of the eccenca Corporate Memory – GDPR Solution Package

Organizations' opportunities

From an internal perspective GDPR can serve as a wake up call to good data governance practise beyond the scope of personal data. The internal project can be

designed to resolve a much broader scope of issues than only personal data management. The regulation asks controllers and processors to know what they do and what they have in terms of data. This is a valuable good practice that can improve the agility of organizations on all levels. Markets change faster than ever. Being able to adapt requires a critical level of introspective capabilities. If a company wants to change processes, it needs to change systems and related data, too. The better data governance and in turn data management are in shape, the higher the probability to successfully manage the general digitalization challenge that all sectors currently face.

From an external perspective demonstrating good personal data management is ever more important to win and keep the trust of customers. With GDPR the sensitivity to good data protection will keep growing on the consumer side. Companies that fail to address this aspect will sooner than later notice that their customers were given a powerful stick to beat back, they never had before. On the other hand, companies that demonstrate that they actively care for data protection will see a competitive advantage, because data protection will be perceived as important by a growing segment of their target groups.

Conclusion

The General Data Protection Regulation puts the rights of the data subject in its core of requirements addressed to data controllers and data processors. Data controllers and data processors are made accountable to care for personal data. It is obligatory to companies to know each and every step of data's lifecycle and the impact of daily business on data management. Now that companies also have to prove being compliant with the new rules, it is important that they know which data management process is affected by which specific GDPR articles.

A Final Word

The objective of this book was to show the true value of RegTech in a practical setting. The new rules introduced by the GDPR are a perfect example for a use case that explains the opportunities of a RegTech solution rather than talk about RegTech in abstract terms. We have seen that our RegTech example, eccenca's Corporate Memory, supports key functions of personal data management by operating a comprehensive framework, which relates data to procedures, systems, and regulation. We've seen how innovation in the form of semantic technology helps to significantly reduce and effectively manage complexity, simplifies management of data, reduces operations' costs and cost of risk. The outcome is impressive: transparency, reliability, trust and performance will increase organizations' competitive advantage. Besides the obligation to adhere to the GDPR eccenca's technology opens up opportunities to support a broader range of data governance and data alignment initiatives, beyond the mere scope of GDPR.

GDPR is one of the most challenging regulatory initiatives of recent times. When done right, it is a huge opportunity to win trust of customers, creating a substantial competitive advantage in a crowded field.

About

PlanetCompliance is the leading platform for insights and in-depth analysis on Financial Services Regulation and Innovation. It's the go-to-source for everyone interested in FinTech, RegTech or Blockchain and how compliance impacts business and viceversa. For more information, go to www.PlanetCompliance.com

eccenca is a software and solutions company. eccenca's next generation data management solutions are driving automation and rationalization for metadata management, data integration, analytics and data driven processes. By turning 'strings into things', eccenca is creating meaningful and machine interpretable knowledge graphs that allow the integrative interpretation of previously siloed data across the enterprise or even throughout value networks. To find out more, go to www.eccenca.com