Lux Magi

RapidGen

How GDPR Makes the Case for Decision Management

Introduction

The General Data Protection Regulation (GDPR) will revolutionize the way in which most companies with partners or clients resident in the European Union source, handle and distribute their data. Further, it gives new rights to EU citizens that are the subjects of this data. The biggest revolution in data handling compliance since the original 1995 Data Protection Act (DPA), GDPR will force medium and large companies to appoint new, independent personnel charged with monitoring data processing and servicing the rights of data subjects. It also sets record fines if these regulations are not followed. With a target implementation date in May 2018, many companies are concerned about their ability to meet this regulatory standard.

Crucially, GDPR will impose new obligations on companies that will require new levels of transparency in their decision-making, necessitating the increased use of techniques such as decision management and modeling. For example, under some circumstances, GDPR will make companies responsible for explaining their automated decision making when challenged by data subjects who are affected by the outcome. We examine these new obligations and describe how GDPR helps make the case for decision management.

What is GDPR?

GDPR is a new compliance mandate that will impact the majority of companies that store, move or process data from, or involving, a European company or involving subjects domiciled in the EU. A stronger replacement for the Data Protection Act of 1995, GDPR will be enforced from May 2018 and will have a wider territorial scope, more obligations, be better harmonized across Europe and will have the backing of every EU state. Most significantly, it will entail much more punishing fines for non-compliance: 20M Euro or 4% of annual turnover, whichever is the larger—such fines are enough to compromise some companies.

Many make the mistake of assuming GDPR only controls European companies, but this is far from the truth. GDPR has jurisdiction over corporations processing data in the EU. However it also encompasses any company handling the data of EU subjects (persons or companies) or supplying services or goods to the EU regardless of: where it is based, whether or not money changes hands and whether or not the data processing takes place in the EU.

GDPR has the power to ensure that:

- companies do not hold excessive data;
- they hold data only for lawful reasons;
- they do not collect or distribute it without active consent of the subject;
- they have more stringent security, processing and breach control/reporting protocols controlled by documented personnel within the company (the Data Protection Officer and the Information Security Manager); and
- they uphold key rights of data subjects, including the right to have inaccurate data corrected, to prevent data being used for direct marketing without their active consent and the right to have their data erased (to be forgotten).

Although GDPR will only affect medium and large sized companies (normally those with 250 or more employees), it cannot be evaded by sub-contracting out these responsibilities to subsidiaries or business partners as the DPA could. Its central obligations must be provided in-house after an extensive information audit to assess the company's information assets, regular privacy impact assessments to ensure data streams are being handled appropriately and a demonstration that the company has the right to hold and process the data it does. Companies will be responsible for checking and documenting the adequacy of data suppliers to meet these needs and ensuring the physical location, security and integrity of the data.

How Does Decision Management Support GDPR?

Decision Management is a means of bringing a company's decision-making 'into the light', to make decisions an explicitly-managed, corporate asset. Specifically decision management:

- identifies and prioritizes operational decisions and their impact on the business;
- makes operational business policies transparent and accountable to all stakeholders by representing complex logic in easy to understand formats such as decision tables;
- renders decisions accessible to business experts and analysts for rapid innovation and improvement;
- checks their integrity and drives out all their data dependencies;
- helps to explain, after the fact, why a decision generated a specific outcome and
- confirms that they are used consistently and reliably.

Decision Modeling is a vital part of decision management: it gives us a standard means of representing business decisions—The Decision Model and Notation (DMN)—that is much easier to understand than code or ad-hoc spreadsheets, that is a safer representation for business policies than leaving them in the minds of subject matter experts and, most importantly, that is directly executable. This means that decision models can be tested and deployed without the need to develop decision-making code. DMN enables a viable, model-driven approach to decision-making and evolution, allowing you to convert decision models into automated, highly-efficient decision services without needing to go through the error-prone and time-consuming process of translating decisions into programs.

So how does this help with regulatory compliance mandates like GDPR?

Decision Transparency and Article 22

Article 22 of the GDPR demands that subjects (an individual about whom a company holds information) be safeguarded against potentially damaging decisions being made on their behalf, or concerning them, without human intervention. Business operations that are fully automated and that have outcomes that could disadvantage a subject or 'have a significant or legal effect on them' (e.g., determining if someone is eligible for a mortgage or a credit card) must support the following entitlements:

- The subject has a right to obtain an explanation of the decision and its consequences
- The subject has the right to express a view on the decision and challenge it

These rights are only waived if: the decision was required for entering or remaining in a contract with the data subject (and therefore the decision-making and its consequences are spelled out in the contract); it is authorized by law; or it is based on explicit, active consent by the subject.

Furthermore Article 22 of the GDPR stipulates that in circumstances where it is acceptable to profile a subject (e.g., for the purposes of targeting goods and services, determining the best next action or cross-selling), such profiling must be transparent. Specifically: the profiling logic must be meaningfully described; the subject must be aware of the consequences; companies must be able to demonstrate that appropriate logical, mathematical or statistical approaches have been used and they must prove procedures are in place to spot inaccuracies or mistakes.

Decision modeling offers a powerful means of supporting all these rights because it offers the most effective means of documenting decision-making in a transparent, open-standard format currently available. This standard, DMN, allows even the most convoluted decision-making to be represented transparently using straightforward layouts free from jargon and code. Furthermore, many decision management systems provide an after-the-fact explanation of decision behaviour, giving a blow-by-blow account of how and why an outcome was determined and all the data used. This powerful combination allows data processors to explain their automated decision-making in easy to understand terms, using decision tables and other accessible representations to answer subject queries. It helps them meet their obligations while at the same time giving them a framework to improve their automated decision making.

Being Explicit About Data Sources

GDPR insists that companies perform a one-off information audit and regular privacy impact assessments. Both require a thorough understanding of the exact source of all inbound data and why and how it is used to support automated decision-making. Companies need to understand how their decisions depend on data—down to the level of individual fields. They also need to know what implications this use has on the GDPR compliance of their operations and the data's completeness and latency requirements. This knowledge is essential for two reasons. Firstly, the degree of sensitivity of some data fields, currently classified into one of four levels, determines if and how the data may be used for a given application; the use of sensitive attributes is severely restricted. Secondly, the constraints on which data may be used may change with future versions of GDPR or with alterations in the purposes for which the data is used.

Decision modeling explicitly captures the dependencies that decision-making has on data and business knowledge. Many companies use decision modeling precisely because it enables a quick and thorough audit of what data is required and why. Furthermore, many decision modeling tools can support queries on how specified fields are used across the enterprise and the big-picture impact of restricting or eliminating the use of specified data fields.

The strict accountability enforced by a decision management environment is also vital for thorough and transparent information audits and the sensitivity classification of data attributes.

Ability to Support Decision Complexity and Rapid Change

Like any new compliance mandate, GDPR has many geographical and jurisdictional variations and uncertainties. A good example of this is the rights young people have regarding how their sensitive data are used under the regulation. Specifically, how age is used to classify minors and determine the degree to which they can personally give consent, as opposed to their guardians. The age boundaries used depend on the nation of jurisdiction. Also, the mechanics of parental consent in the current version of GDPR is recognized as draft and is likely to change post go-live. These factors mean that any automated support for GDPR must be capable of expressing these variations and accommodating change quickly and safely.

Decision modeling is an ideal means of documenting complex decisions because it scales effectively and it is expressly designed to support jurisdictional and other variations. Decision management technology stacks support the rapid evolution of regulatory logic through the transparency of decision models, provision of a collaborative environment with change impact assessment and the fact that models are directly executable. Further, the regression testing facility that many stacks provide ensures that regulatory updates can be performed quickly and without error. We refer to this combination as **safe agility**.

Conclusion

Many compliance directives benefit from decision management, but GDPR undoubtedly represents one of the most onerous regulatory mandates of the past decade—the first to explicitly demand an after-the-fact ability to explain your decision-making but certainly not be the last. If your company falls under the scope of GDPR, using decision modeling, deploying a decision technology stack and executing your automated decisions on a highly performant decision execution engine are vital requirements to success.

About the Author

Jan Purchase has been working in investment banking for 19 years, the last 13 of which he has focused exclusively on helping clients structure their requirements and automate their financial processing with business decision management, decision modeling, business rules management and business process modeling. He is a founder of Lux Magi Financial Rules, a company specializing in delivering, training and mentoring all of these concepts to financial organizations. Lux Magi has been applying business decision modeling and rules to the automation of financial processing and regulatory compliance for over 14 years. In December 2016, Mr Purchase published a book Real World Decision Modeling with DMN with James Taylor which addresses many of the topics discussed in more detail.

Lux Magi

Lux Magi helps investment banks and other finance companies worldwide to leverage the power of business decisions, business decision modeling and business decision management to develop, manage, automate and optimize their business policies and compliance procedures.

Lux Magi believe that systems that deliver business benefit can only do so if they are controlled effectively by the business.

RapidGen

RapidGen has a long history of Decision Logic programming using the concise and transparent format of Decision Tables as the basis of its own programming language, RPL.

RapidGen's expertise in enterprise class applications is now being applied to the development of a powerful, highly scalable execution engine for decision models, particularly DMN (Decision Model & Notation).