GDPR & Beyond

The Real Business Drivers of Data Compliance

Introduction

There are clear drivers for compliance with GDPR which stem from a defensive position whether by a Public or Private Sector entity. The Sanctions in the form of fines as well as reputational damage are frequently stated as instigators of action to adopt the Regulation and parallel national legacy Data Privacy law. However, at Micro Focus, our 2 year program on assisting our clients with GDPR technical effectiveness has revealed a much broader set of both tactical and strategic rationales for engagement. They can broadly be grouped into Compliance, Operational Efficiency and Revenue.

The following examples are all taken from Micro Focus® client commentary in terms of the "Business Value" to be gained—as opposed to the eventual technical solution they might need.

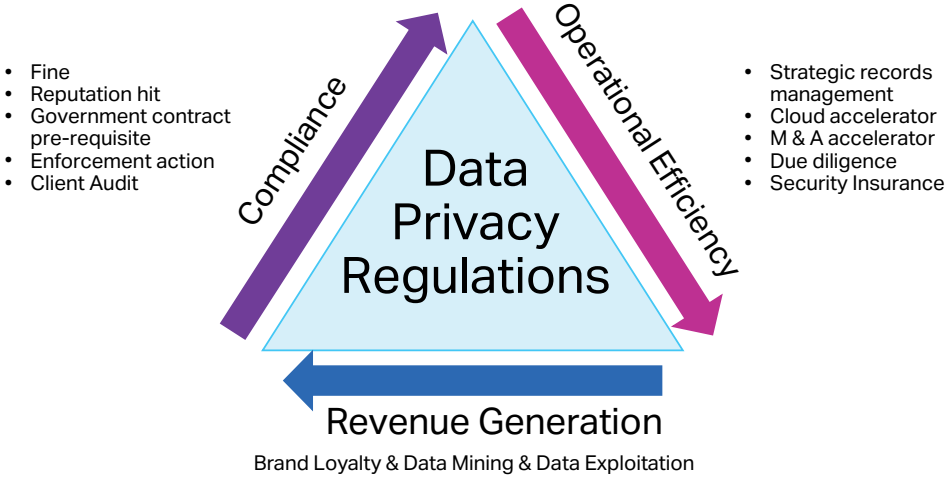


Figure 1. Compelling business logic for GDPR Compliance

Compliance

In terms of gaining senior management attention, the downsides and risks of non-compliance are obvious. Though the cases we cite below indicate that GDPR compliance is an issue affecting almost all departments & sponsors, not simply the CIO / CISO / Compliance departments:

a. **Real reputational damage.** GDPR has 2 fundamental challenges of both Security standards and Data Life Cycle Management. Even without Regulator intervention, the 2011 hack into Sony, with 77 million customers data prejudiced, resulted not in a fine as such but rather in the 30% fall in their share price—so a real issue to capture the imagination of senior management. A recent commentator on this opined that "Cyber risk is stronger than records management risk." One can agree—but both risks are enhanced by GDPR—and of course one cannot encrypt/protect data until one has identified it.

b. **Remediation cost.** A similar instance of hacking impacted the UK Talk Talk telco in 2015 accessing 156,959 customers' details. While the Regulator fine was £400,000, the cost of security systems / software mitigation created a demand for over £40 million in expenditure. Hence the negative financial impact should not always be seen in the area of the fine.

c. **Client Audit.** A number of UK & Irish universities point to a GDPR negative impact which probably impacts all private sector entities. At the core of the GDPR logic is that of the ability of a customer to trust the service / goods provider with their data. So if one cannot demonstrate that one is "GDPR effective," however that is defined, then one is simply going to lose business. In the case of Universities, one in Ireland advised that more than 60% of their revenue comes via research sponsorship from overseas in particular. While such funding has always had legal / regulatory pre-conditions, these now include GDPR. So a significant impact of non-compliance can be negative financially.

d. **Government tender pre-requisites.** We have also learned of GDPR demonstrable effectiveness being an essential element of Requests for Information / Proposals pre-conditions of bidding on public contracts. As with the universities, this could significantly impact day to day commercial business acquisition—a long way from fines and reputational damage.

Operational Efficiency

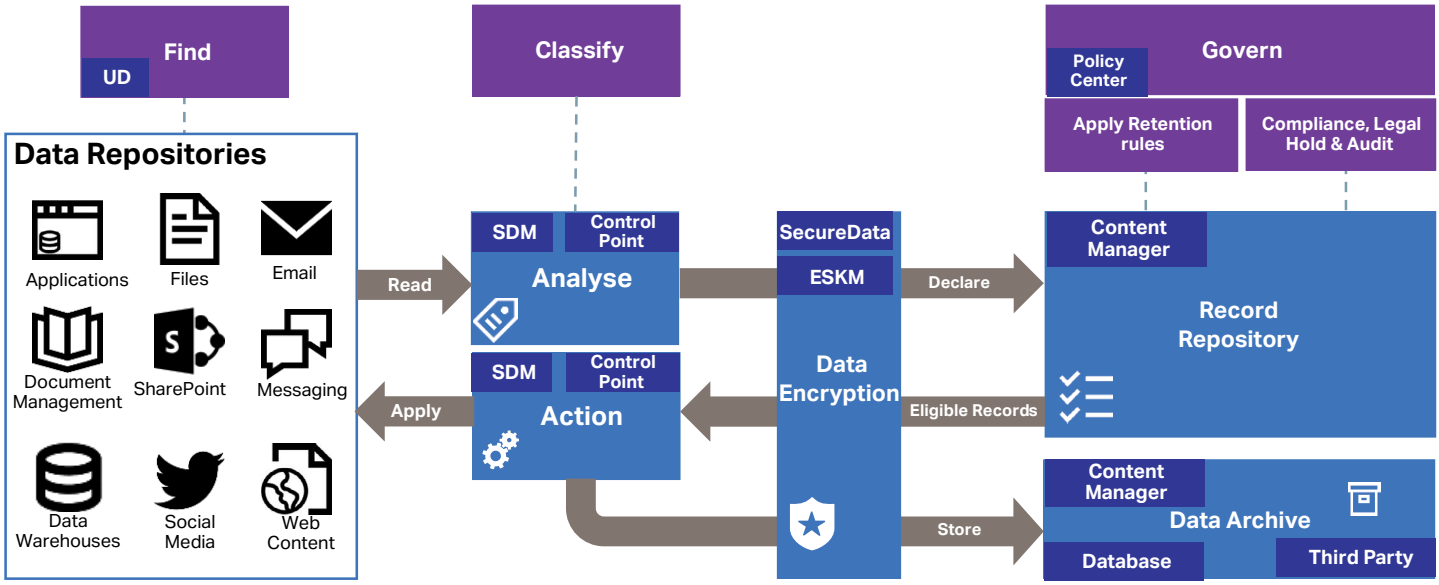
Meeting GDPR expectations requires the significant ability of a CIO to be able to have visibility across their real estate as well as ability to extract essential data at speed to meet SAR requests and GDPR task execution e.g. right to be forgotten, data portability. This involves a strategic capability for data management and security which the GDPR legislators could not have imagined. While providing a downside challenge, it is interesting that many major corporations are actually turning compliance into a positive advantage:

a. **Legacy Data Cleansing.** "If you're looking for a needle in a haystack, reduce the size of the haystack." For the CIOs of 2 global insurance companies, the task of finding a single individual's data—in any format, in any location within the company, within 28 days was impossible. But why? Because they simply were not in touch with all their legacy data silos—nor the multiple data types. Micro Focus' own experience is that more than 30% of corporate data on average across the private Sector is "dark data"—meaning simply unknown as to location and content. To get to the GDPR information, stripping out the unwanted data would make life so much easier. Hence getting rid of the Redundant / duplicate, Obsolete / time expired and Trivial data ("ROT") would actually accelerate access to the essential record needed to run and advance the business. The 2 CIOs also recognized that such cleansing could product an ROI in the form of reduced backup / archive / storage costs which could help pay for new technology enabling compliance.

b. **M & A acceleration.** The head of governance at a global energy company commented that her biggest headache in facilitating new corporate disposal / engagement was the personal data of employees / customers / 3rd party agents. If GDPR adherence would cause the company to have such Personal Data immediately available and capable of indexation and processing, this would actually accelerate her M & A business

c. **Cloud acceleration.** The CIO of another global energy company is in process of migrating global data from on premise into the cloud. GDPR requirements of accessibility and audit trail caused them to consider whether they were able to find such data at speed. And why not? Because of the ROT existing. Hence GDPR could act as a catalyst for the deletion of useless data before migration to the cloud—thereby reducing their eventual cloud storage costs.

d. **Security Insurance cost-saving**. Commercially, the security non-compliance under GDPR is arguably more visible than the Data Life Cycle Management cases described above. But the regulations such as Article 34.3 directly indicate that the use of "appropriate technical and organizational protection measures" will mitigate the needs to inform a data subject of a breach within 72 hours, Whilst this is one aspect of cost saving, carrying out a Security audit for a major German electronics group can also



UD: (Micro Focus ITOM) Universal Discovery
SDM: (Micro Focus IM&G) Structured Data Manager
ESKM: (Micro Focus Data Security–Atalla) Enterprise Secure Key Manager

Figure 2. C=GDPR readiness reference architecture

reduce the cost of cyber insurance premiums. It is now common for insurers to offer to make such accommodation, provided a risk assessment of the insured and its existing technology is effectively carried out. So consideration of key security aspects can actually provide costs savings when considering:

1. Entity overall security
2. Application security through penetration testing
3. Data base security in terms of in built data masking
4. Pure data security through anonymization, pseudonymisation and encryption; and
5. Personnel security through improved Identity Access Management.

e. **The Swiss Army Knife for compliance.** A global Asian Bank has found a great opportunity for recycling an existing compliance solution. Back in 2010, to comply with the USA Dodd-Frank Act, their investment banking dealing rooms needed to be able to re-construct a derivative trade within 72 hours—over potentially the next 30/40 years! Hence they acquired technology to locate multiple data types/mass unstructured data, classify it via its metadata, and then apply such an evidential task. What the CIO then had as a "lightbulb moment" was the realization that he had acquired a multi-purpose "policy enforcement" tool. Since then, he has been applying it to MiFID, EMIR and of course now GDPR. And the natural extension is that this combined Data Life cycle Management facility can be used for virtually any regulatory, legal or corporate standard to be imposed in the future. In March 2018, he advised that its effect in reduction of ROT, storage costs and man power has been some "$20–25 million per year."

Revenue

The most unexpected upside benefit from GDPR compliance comes from the ability to improve competitiveness and hence revenue generation. Only recently, the UK ICO has advised: "The ICO's approach is designed to help create an environment within which, on the one hand, data subjects are protected, while ensuring that, on the other hand, business is able to operate and innovate efficiently in the digital age."

a. **Customer loyalty and attraction.** A major **Nordic media company**'s Chief Privacy Officer advised that being able to "stamp GDPR effective" on their web site would help provide assurance as to trust in their ability to handle sensitive personal data. Not only for existing clients, but also in attracting new clients. So a competitive advantage can be gained from being early to engage and assure clients.

b **Data mining.** As a consequence of the operational efficiency data cleansing described above, an **Asian satellite navigation manufacturer** has identified a new source of revenue. Not only will they sell the technology to the car manufacturer, but also offer to bring back in the data on a used car, cleanse it, encrypt where necessary and send it back to the manufacturer for future market analysis and new marketing campaigns.

c **Privacy processing as a service.** Similar to the above is the **major European Airport** which is needing to acquire technology to handle its own data life cycle management, policy enforcement and security on GDPR. They then had a thought. They are literally the "spider in the middle of the web." They have multitudes of shops / restaurants and vendors who have Personal data issues who reside on their premises—not sufficiently large to afford their own technology solutions to GDPR. And in addition, there are all the airlines with PNR data which arrive and depart from their location. In which case they are working to acquire a SaaS capability not only to process their own information, but also produce a new revenue stream by means of acting as a Data Processor for those who depend on them.

d. **Local Government self-help.** On the same lines as the airport, large municipalities already provide insourcing / processing capabilities for surrounding smaller community groups. So why not continue the process in relation to Personal Data and GDPR? A **major UK city** GDPR Programme group is already contemplating providing such remunerated service—even if in the form of "wooden dollars"!

Contact us at:
www.microfocus.com

Timing Context

With the GDPR implementation deadline of 25th May 2018 passed, a question must be—"Is this the beginning of the end, or the end of the beginning." One could say the latter given that a Reuters report on 8th May 2018 of a survey of 24 European Data Privacy Authorities found that 17 of them "said they did not yet have the necessary funding, or would initially lack the powers, to fulfill their GDPR duties." If one then links this to the Micro Focus findings across Europe that over 85% of entities are still at the Data Discovery stage, there is much to do on both sides of the Regulation. Perhaps some of these practical instances of business drivers can assist in propelling GDPR Programmes to a successful conclusion.

Learn More

For further explanation of Micro Focus' experience and GDPR gap analysis & solutioning, please visit our web site at **www.microfocus.com/gdpr**.