THE GENERAL DATA PROTECTION REGULATION (GDPR)

5 QUESTIONS
DATA-DRIVEN COMPANIES SHOULD ASK TO MANAGE RISKS AND REPUTATION

Data is rapidly becoming the lifeblood of the global economy.

In the world of Big Data and artificial intelligence, data can offer companies a decisive competitive advantage or one can fail on other risk damage the reputation and bottom line of those that remain unaware before managing it.

Although until recently, the fines for breach of data protection regulations were limited and enforcement actions infrequent.

However, the introduction of a potentially revolutionary European GDPR is likely to transform the way data-driven companies handle customer data by exposing them to the risk of hefty fines and severe penalties in the event of incompliance and data breach.

HOW DOES GDPR IMPACT DATA-DRIVEN ORGANISATIONS?

The GDPR introduces a number of new legislation requirements that will significantly impact the way businesses collect, manage, protect, and share both structured and unstructured data. Few of the most important among them are:

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

➤ It is the process for identification of any risk that might arise when developing new solutions or undertaking new activities that involve the processing of customer data. If the process draws an inherent risk then a Data Protection supervisory authority must be consulted with.

DATA PROTECTION BY DESIGN AND DEFAULT

➤ Implementation of the GDPR will require companies not only to implement technical and organisational measures to protect personal data but also to ensure that measures are continuously reviewed and updated.

VALID AND VERIFIABLE CONSENTS

➤ The GDPR sets out stringent new requirements for obtaining consent for the processing of personal data from customers.
➤ Consumers should read the process of withdrawing a consent as easy as providing a consent.
➤ The consent should be 'explicit' for sensitive data and customers should be provided with a right to object when their personal data is being collected for the purpose of direct marketing.

WHAT ARE THE POSSIBLE CONSEQUENCES OF NON-COMPLIANCE?

Consequences related to non-comply of GDPR are not just limited to monetary penalties but can potentially damage a business' reputation and bottom-line.

There are three factors that together make the GDPR the most stringent regulation in the European data protection regime.

Reputational Risk

This will consequently bring data protection breaches to light, compromising a company's market position and reputation.

Geographic Risk

All organisations offering goods or services to EU markets or monitoring the behaviour of EU citizens are subject to the GDPR. This includes offshore analytics companies as well.

Huge Fines

Failure to comply with the new regulations will lead to significant fines of up to 20 million EUR or 4% of the company's global turnover, whichever is higher.

To avoid the huge fines and severe penalties, businesses will be required to revise their entire data governance approach in order to stay compliant and mitigate reputational and financial risks.

5 QUESTIONS TO
ADDRESS AND MITIGATE THE RISK OF NON-COMPLIANCE

1. How can I minimise risks and protect my business' reputation?
2. How can my business protect personal data?
3. How can my company implement technical infrastructure that will ensure optimal governance of client data?
4. How can my business uphold these new regulations and define client data collection and storage?
5. How can my business handle different types of data streams?

① How can I minimise risks and protect my business' reputation?

Taking the following measures can help you ensure your compliance to the new data protection legislation.

DEFINE PERSONAL CLIENT DATA

Document what personal data your company holds, where it came from, and where you share it with to ensure compliance. Begin with a thorough review of your existing database.

MANAGE DATA STREAMS AND PROCESSES

Develop a roadmap to determine your sources for data input, processing and sharing with other businesses. Now evaluate their compliance to the new regulations, and take adequate measures to ensure good data governance.

DESIGNATE A DATA PROTECTION OFFICER

Designate a Data Protection Officer who has the knowledge, support, and authority to assess and mitigate non-compliance risks.

ENSURE SWIFT RESPONSE TO WITHDRAWAL REQUESTS

Respond efficiently to the customers' withdrawal consent and update the system to flag that the user has withdrawn consent so as to prevent further direct marketing.

② How can my business protect personal data?

To ensure the security and confidentiality of the now defined categories of personal data, businesses can use the following measures:

ADOPT A 'PROTECTION BY DESIGN' APPROACH

There are certain 'protection by design' techniques that businesses can use to protect the personal data of their customers. These include:

PSEUDONYMISATION

It involves categorisation of the personal data of customers into two types so that one type can no longer be attributed to an individual unless accompanied by the second type of information which is kept separately and is subject to various data protection measures.

DATA MINIMISATION

As the name implies, data minimisation is about ensuring that only the data that's necessary for a specific purpose is processed, used, or stored.

ENCRYPTION

Encryption can help transform personally identifiable information into personally non-identifiable information by converting it into a code.

③ How can my company implement technical infrastructure that will ensure optimal governance of client data?

GDPR not only requires businesses to implement a well-built and foolproof infrastructure but also directs them to continuously review and update the infrastructure.

ALIGN DATA & ANALYTICS STRATEGY WITH POLICIES

Businesses should focus on developing a data and analytics infrastructure that's CONTROLLED, PORTABLE, and COMPLIANT.

- Data collection should be purpose driven.
- Data collected with the consent of clients should be kept in self-controlled storage and processed according to all applicable data protection regulations.
- Customers should be provided with a right to object to data collection and processing for direct marketing processes.

COMPLIANT DATA & ANALYTICS ARCHITECTURE

CREATION & COLLECTION (company regulated)

ANY SOURCE

DATA PREPARATION FRAMEWORK (company regulated)

CONTROL | PORTABLE | COMPLIANT

PROCESSING & STORAGE

Analytics node | Report node | ERP node data & metadata | Storage node | System node

ANY APPLICATION

UTILISATION

Analytics Applications | Client channel reporting | Branding Applications | Billing & advanced analytics applications

MANAGE DATA LINEAGE

Certain data governance solutions organised by leading tech companies help businesses adopt:

➤ A standardised approach to discovering their IT assets and define a common business language to ensure optimal policy and metadata management.
➤ Create a searchable catalogue of information assets.
➤ Develop a point of access and control for data stewardship tasks.

④ How can my business uphold these new regulations and define client data collection and storage?

To enhance the compliance of their client data collection and storage processes, businesses should seek assurance from a data protection officer who can:

- Advise and advise the business about its obligations pursuant to the regulation.
- Monitor the implementation and application of adequate data protection policies.
- Ensure optimal training of staff involved in data collection and processing operations.

Designating a data protection officer can also help businesses monitor and classify their incoming data streams to get client's approval regarding how to use data.

⑤ How can my business handle different types of data streams?

Data stream management software is a viable solution to this challenge. A data stream manager allows businesses to:

➤ Collect and distribute data in a private and compliant way.
➤ Reduce costs and complexity in data life cycle management.
➤ Have real-time access to all structured and unstructured data via the cloud or on-premise.
➤ Centralise all data sources for improved visibility and control.
➤ Develop a controlled environment for data-driven operations.

With a data stream manager, Data Protection Officers can define privacy levels, manage user rights, get an insight into how their data is being collected or used, and more.

CONCLUSION

Many of the GDPR's principles are much the same as the current data protection regulations. Therefore, if your business is operating in compliance to the current law, you can use your current approach to data protection as a starting point to build a new, more robust and secure GDPR-compliant data protection infrastructure.

To learn more about GDPR compliance, subscribe to the educational webinar taking place on April 3rd, 2017. The webinar will be hosted by BrightTalk and presented by Primeur and Lane and Space do Vivas.