Get on Top of Privacy Regulations with a Unified Data Fabric

By, **Tim Healy, Esq**.
COO, YOUnite Inc., tim@younite.us

Introduction

This is not another white paper scaring you about the potential fines from the GDPR, but rather to convince you to see this challenge as an opportunity to improve your data ecosystem and thereby improve your clients' experience and your company's bottom line.

There is an old saying that adversity presents opportunity. And many see the European privacy laws as a major data management headache. New rules about getting customers' permissions to use their data, managing where the customers' personal data can be geographically stored, ensuring the data is current, material and accessible may seem onerous. No doubt it is a challenge, but isn't it also a good business practice to have good clean consistent data? I like to think with better data comes better business decisions, regardless if legal compliance issues help to drive us in that direction.

55% of all data collected by companies is unused (Splunk global survey reported by Priceonomics Aug. 2019).

The real challenge is gaining control over the vast amount of enterprise data that is in the company's source systems, whether it is in the cloud or on premise.

Using the carrot and stick analogy, the ‘stick’ might be GDPR privacy rules, but the ‘carrot’ is having a better understanding of what data you have, where it is, and that it is current and accurate.

GDPR's Trajectory

Ireland

Although we hear about centralizing data as a solution, I don’t think it works in today's fast changing legal environment. Ireland recently provisionally held that Facebook could not process Irish citizens’ personal information in the USA.

> “(Reuters) May 23, 2021 Ireland’s data regulator has given Facebook six weeks to respond to an investigation that may trigger a ban on the social media giant’s transatlantic data transfers following a High Court ruling that the probe could resume."

The case stems from European Union concerns that U.S. government surveillance may not respect the privacy rights of EU citizens when their personal data is sent to the United States for commercial use.

Ireland’s Data Protection Commissioner (DPC), Facebook’s lead regulator in the EU, launched the inquiry last August and issued a provisional order that the main mechanism Facebook uses to transfer EU user data to the United States “cannot in practice be used”.

Facebook had challenged both the inquiry and the provisional order, saying they threatened “devastating” and “irreversible” consequences for its business, which relies on processing user data to serve targeted online ads.

If the Irish regulator enforces the provisional order, it would effectively end the privileged access that U.S. companies have to personal data from Europe and put them on the same footing as companies in other nations outside the bloc.”

Germany

In Germany in June of this year, the government recently ordered its employees to close the Facebook app because it does not comply with GDPR and German privacy laws.

> “BERLIN, June 29 (Reuters) - German government organisations have until the end of the year to close their Facebook FB.O pages after the data protection commissioner found the social network had failed to change its practices to comply with German and European privacy laws…"

[Commissioner] Kelber added that party line app Clubhouse, video clip app TikTok and Facebook's Instagram site also appeared to have similar shortcomings, and recommended government organisations stop using them too until his inquiry was concluded…

Kelber said it was impossible to run a fan page in such a way that followers' personal data was not transmitted to the United States. Under EU law, personal data can only leave the EU for a jurisdiction with equivalently strict data protection rules, something that is not the case for the United States…” (Reporting by Thomas Escritt)

These certainly are challenging times, but it looks like centralized processing of PII is not a likely solution. I think the better practice is keeping the critical data in source systems in each state or home country; thereby eliminating one large issue with GDPR. And I don’t think you can say, ‘they will work all this out’. I can guarantee that rules and regulations will change over time as regulators and lawyers argue so data and governance systems must be agile.

Even companies in Great Britain must remain agile. As you know, Great Britain was part of the EU and so was within the GDPR agreement for sharing data…until it wasn’t. When ‘Brexit’ passed, Britain was no longer part of the EU or given special privileges under GDPR. All British companies were in limbo if EU countries could share data with British companies. There is presently a tenuous agreement that if Britain follows the GDPR rules in spirit then data sharing will be allowed. However, the independent minded British are thinking of making ‘better’ privacy rules and if they do it could put British companies in jeopardy of GDPR fines.

Building a Data Fabric With Federated Data Unification

To avoid this kind of legal risk that Facebook and others are having, I suggest you don't centralize your customers' data, but rather keep it in its originating source system. This is called 'Federated Data'.

YOUnite provides real-time data change routing and governance between your enterprise source systems.

PII can be deidentified to enable sharing under GDPR.

With Federated Data Unification, you build a data fabric across your enterprise data tier but still have access to all your data subject to the governance permissions for a particular country or zone. A Federated Data Fabric creates permission zones and with the zones it is relatively easy to react to the changing legal landscape as it happens. If Ireland or Germany changes a rule or interpretation on what is PII or where sharing is allowed, then your data steward can change the fine grained data governance to control the flow of the subject data in or out of Ireland or Germany company wide. If the issue is resolved then the permission gates can be reset under the new guidelines and the data can be shared responsibly.

But let's remember the 'carrot' that we are after is to have better control over our business data. The 'stick' of embarrassing corporate GDPR fines may have helped move us, but after the federated data unification platform is deployed, your business has access to more of its data, can clean, enrich and update the data in real time as it enters or moves through the ecosystem i.e. a data fabric. And I would suggest that you will have better confidence in your data analytics because you have more confidence in the quality of your data. Again, the opportunity is making better decisions with better data with federated data unification. Good customer service and GDPR compliance will naturally follow.

YOUnite provides Enterprise-Wide Data Quality

- **Clean, enrich and transform data across the enterprise**
- **Choose best-of-breed data quality tools to integrate into the data unification workflow**
- **Extend existing investment in existing data quality solutions**

What is GDPR?

The General Data Protection Regulation, or GDPR, aims to assert the rights of EU citizens on their privacy and personal data and highlights the responsibility of businesses doing business in and with the EU in handling the personal data of their citizens. Your business does not have to be in Europe. An American business that markets to, or provides services for, EU customers falls within the European privacy regulations.

Under the GDPR, individuals have certain rights to their personal information. These are:

- The right to access
- The right to be forgotten
- The right to data portability
- The right to be informed
- The right to have information corrected
- The right to restrict processing
- The right to object
- The right to be notified

Ask yourself if your data management systems, individually or collectively, can respond to these customer demands.

The GDPR Has Made Companies Fiduciaries of Customer Data

The hard part for some is the realization that there has been a paradigm shift as to who owns the customers' PII data. The GDPR clearly gives individuals, prospects, customers, contractors, and employees more power over their data and takes away power from organizations that collect data for monetary gain. Failing to comply with this new world view on PII will leave businesses facing hefty fines,

YOUnite is a firewall for your data fabric:

- **Fine-grained real-time data governance provides the tools needed to control the sharing/restricting of data**
- **Granular control of sharing at the data property level (e.g. PII)**
- **Simplifies sharing/ restricting data from a single dashboard**

which can amount to 4% of their annual global revenue, or 20 million Euros, whichever is greater.

This means organizations need to have strict control of the systems and processes that they use to collect, manage and share information about their customers, employees, suppliers and other parties that they do business with.

The challenge for businesses is that the growing amounts of data has resulted in fragmented data spread throughout the business data stores and having it obscured behind departmental silos with each department potentially collecting and using the customer data in its own way. Without a holistic approach to the data in the ecosystem, it is a real possibility that a business will have multiple records of the same customer without knowing it. In the context of GDPR, how could the business respond to a customer demand for their data if the company does not know where that customer's data is?

The solution is unifying the important data in the enterprise under one ecosystem. I don't mean having the data physically centrally stored, but logically connected together...a federated data unification. The data stays in the source system it was created in (and stays in the legal jurisdiction required under GDPR or other governmental regulation) and a federated data unification platform can aggregate all the customer's data in order to comply with a GDPR request. Additionally, the real time federated data unification can then provide fine grained data governance to control the sharing/restricting of data as required by GDPR.

There is no need to make copies to a central store or create another point to point integration solution.

Know Where the Data is and How it is Shared

GDPR mandates that organizations processing personal data of an individual must disclose to the individual key aspects such as the scope of data collection, the purpose for data collection, the duration of data retention and if data is being shared with any 3rd party. If individuals agree to share their private data, the organization must ensure that the collection and use of it strictly abides by what the individual has consented to. This can be extremely challenging for organizations that do not have the tools and governance processes to pinpoint exactly where the data resides, when it was created, who has access to it and how it's being used.

YOUnite Shows Complete Federated View of a Data Record's Lineage:

- Single-pane view of all **data change history** across the entire enterprise
- Greatly simplifying the ability to **trace errors back to the root cause** or where it was replicated
- **Data audit time saved** and the process is greatly simplified

The answer is having ***fine grained data governance*** and the ability to track and document the data record lineage. Auditors can then confirm that the company was complying with GDPR.

Right of Access and Right of Erasure

GDPR changed the paradigm on customer data being 'company data on its customers' into the customer's data held in trust by the business. To further that paradigm shift, GDPR also states that customers have the right to request and obtain their data collected by organizations (data processors) and in certain conditions demand that their data be erased.

YOUnite can be implemented to enable global delete policies to data records.

A well organized federated unified data system will know where the data is and be able to aggregate it in reportable form. If the customer's information is found to be stale or incorrect the data can be corrected in the applicable

source system and the updated information can be appropriately disseminated throughout the ecosystem. Similarly, a customer request for deletion can be done from a single user interface over the entire ecosystem, as well as all other business applications where the customer data was shared.

Conclusion

Compliance with Data Privacy regulations is one of the pressing business imperatives for organizations, where non-compliance means significant penalties by regulators as well as lost revenue due to customer attrition. But let's see the opportunity this presents. Businesses are collecting terabytes of data, but according to recent surveys executives believe they are not leveraging 55% of that data in their own systems. This is a lot of unleveraged business assets.

Companies need a strategy that can be implemented over time with the least amount of disruption to the business operations that unifies the enterprise data. No expensive rewrites of the data architecture or the need for another source system to maintain.

Please talk to us at YOUnite, Inc. about what we can offer you as part of an overall GDPR solution and the business opportunities a federated data unification platform can bring you. We can help turn this challenge into a business opportunity.