THE OMNIINDEX FHE BLOCKCHAIN SOLUTION FOR REGULATED DATA

A 2022 OMNIINDEX WHITE PAPER

1 (650) 297-4682 www.omniindex.io info@omniindex.io

Data is becoming both more important in modern business, and more regulated with it crucial that personal and private information is protected and remains confidential. While important, these regulations have made it increasingly difficult for companies to analyze and distribute this business critical data - from Personally Identifiable Information (PII) including protected health information (PHI), through to business secrets.

This paper offers an entryway into these regulations and the challenges they present before introducing The OmniIndex as a potential solution for the secure storing and processing of regulated data with its innovative FHE blockchain.

WHY HAS DATA REGULATION BECOME SUCH A CHALLENGE FOR ORGANIZATIONS?

We are currently in a data revolution as regulators strive to catch up with the needs of modern business in an ever-evolving environment of information monetization and exchange. There are currently over 120 countries in the world who have already engaged in regulating data and there are also further regulations within both different industries, and different types of data.

What's more, experts predict this number is only going to increase.

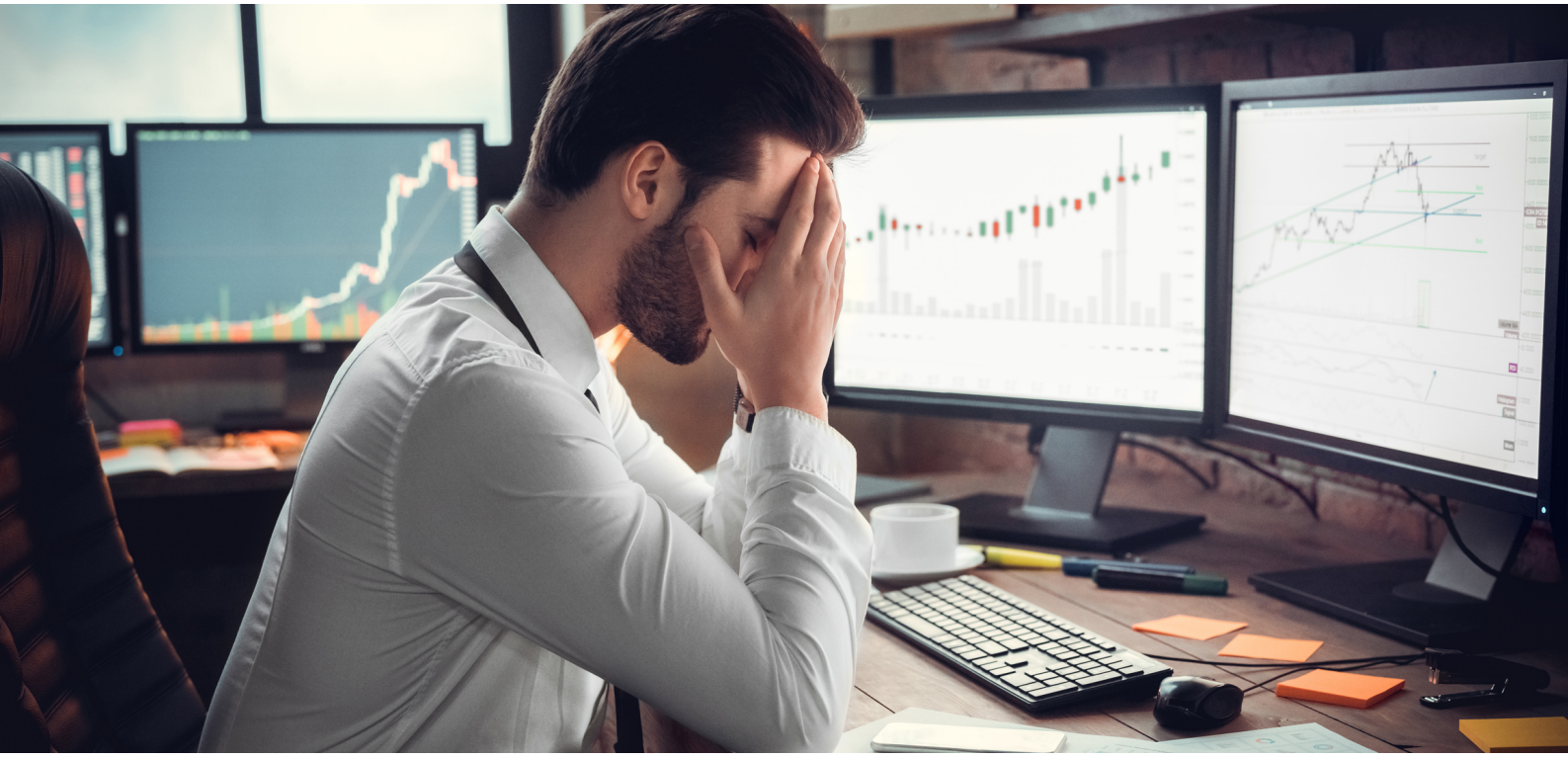
While there is widespread acceptance that regulation is needed with all of us having data that must be protected, both at a private and professional level, these new regulations are causing issues. This is because big data is integral to how modern business works with analytics and distribution at the heart of both decision making, and profit.

As a result of this dependence, any new restrictions have an immediate impact with organizations having to make decisions over how, or indeed if, they can continue storing, analyzing and distributing the sensitive data they hold.

The Global Legal Group's 2021 International Comparative Legal Guide into Data Protection explores this problem. While the study notes the need for the regulations, it also argues that the uncertainty around the ultimate direction and parameters of these new and future regulations is causing a gulf in technological progress being made in different industries:

> "Some businesses have started to take the view that the cost of satisfying such strict privacy compliance obligations is too high to justify, until the product is well established. As a result, users located in jurisdictions with strict privacy laws are increasingly finding that the latest technologies are not available in their jurisdictions."

https://iclg.com/practice-areas/data-protection-laws-and-regulations/1-the-rapid-evolution-of-data-protection-laws



Even when the technologies are available, they are often priced highly to reflect both the need for the product, and the fact that there is a reduction in competition as a result of the difficulty. This means that the gulf noted at an industry level could potentially be seen at an organization level too with less companies able to invest in the costly new technologies needed in order to continue distributing and analyzing sensitive data.

This data is a valuable addition to workflows with it offering both direct and indirect monetization opportunities through optimization insights and enhanced planning models.

As a result, those unable to invest in the new technologies are potentially left at risk of fines if they fail to adhere to regulations and continue analyzing the data, or of being left behind by no longer having the same analytic output available.

While the increasing regulations are causing a challenge to businesses, they are also acknowledged as necessary because of the ever-increasing number of data breaches caused by attacks and data mismanagement. IBM's 2021 'Cost of a Data Breach Report' offers a comprehensive study of these attacks and data losses.

The study recorded a 10% increase in average total costs related to a data breach. As per the report:

> "Data breach costs rose from $3.86 million to $4.24 million, the highest average total cost in the history of this report. Costs were significantly lower for some of organizations with a more mature security posture, and higher for organizations that lagged in areas such as security AI and automation, zero trust and cloud security."
>
> https://www.ibm.com/downloads/cas/OJDVQGRY

The report does offer some hope for businesses too, however, as it states a clear difference between those who are reacting and developing their big data management to face the modern challenges, and those who are not. And, while it is important to note that having strong security in place for confidential and valuable data can be achieved without regulation compliance, it is also true that those who follow the guidelines and protect their data to higher levels of security are generally in a stronger position against such attacks and breaches.

In summary, it is clear that in order to not be left behind it is imperative that organizations get to grips with data regulations and adopt recommended security and data management systems. If they cannot, then they do not just leave themselves vulnerable to more costly data breaches, but may find themselves falling behind the competition with others able to analyze and distribute data that they cannot.

The next section of this paper surmises the key principles at the heart of modern data regulations, including the focus on data lawfulness, integrity and confidentiality.

WHAT ARE THE CORE PRINCIPLES IN THESE REGULATIONS?

While there are a huge number of different data regulations across the world, there are a number of key similarities between them. This section introduces the largest of the regulations and looks at what the core ideas are within them.

The General Data Protection Regulation (GDPR) of 2018 is commonly seen as the keystone in the current big data revolution.

Since Brexit, there is now a separate UK GDPR and EU GDPR. However, while there are differences between the two with the UK GDPR accommodating local law, the two remain fundamentally the same regarding the key principles.

The GDPR is important because it and its seven principles have influenced a number of other key international data regulations. These include Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and India's Personal Data Protection bill.

Likewise, it has heavily influenced the California Consumer Privacy Act (CCPA). This is an important model to consider as, along with GDPR, it is now being used as a template in the development of further regulations - particularly in North America, but also elsewhere.

There are a number of crucial differences between the two sets of regulations surrounding who they apply to, the types of data that are protected, and the definitions over what constitutes data collection, data selling, and data processing.

However, when it comes to data security and the requirement for protecting data's privacy and integrity, the two are much closer aligned. Indeed, it is in fact widely quoted that if you are compliant with GDPR in regards to your data security, then you will also be compliant with the CCPA. However, as is recommended within many of the regulations, it is advisable to seek legal and expert advice on a case by case basis to ensure an organization is compliant with any and all relevant regulations.

Finally, there are also a number of key similarities between the GDPR and the hugely significant Health Insurance Portability and Accountability Act (HIPAA). This legislation ensures healthcare providers and businesses associated with HIPAA-covered entities must adhere to a number of safeguards to protect sensitive personal and health information of a private and confidential nature.

Just as with the GDPR, there is a focus on the security and privacy of personal data. For example with both sets of regulations a company needs to have in place controls for access to sensitive information, methods for detecting unauthorized changes to the private information, and there is a requirement with both for certain types of personal and sensitive information to be encrypted at rest and in transit.

Article 5 of the GDPR sets out the seven core principles that are at the heart of the regulations.

The Information Commissioner's Office (ICO), an independent authority set up to uphold information rights in the public interest, outlines the importance of these principles:

While they do not give "hard and fast rules", they "embody the spirit of the general data protection regime" and compliance with these key principles is "a fundamental building block for good data protection practice."

In summary, these seven principles are:

Lawfulness, fairness and transparency

Purpose limitation

Data minimisation

Accuracy

Storage limitation

Integrity and confidentiality (security)

Accountability

The seven principles can be broken down into two different categories to reflect their different focusses. These are:

1: The decisions around the data. For example why and how data is collected and what is then done with it.

2: How the data is then technically stored, processed, and used to action these decisions.

Regarding the first of these two categories, there is a focus on the data being processed lawfully, fairly and in a transparent manner with it collected for specified, explicit and legitimate purposes. In certain situations in order to be compliant to the relevant bodies, organizations will need to employ somebody to monitor this data processing. In fact, this is increasingly a position being filled by organizations voluntarily as data protection officers and data protection impact assessments are seen as useful ways to manage the flow of data and help prevent gaps in data security and management leading to data breaches.

As for the second grouping of the core principles, there is a focus on ensuring data is processed to a high degree of security. As per the GDPR, this means “including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.” What’s more, these measures must ensure the confidentiality, integrity and availability of the systems and personal data so as to ensure a stable infrastructure is in place to manage security risks, protect personal data against attack, detect security events, and minimize the impact of such an attack and potential breach.

WHAT IS THE OMNIINDEX SOLUTION FOR SENSITIVE AND REGULATED DATA?

This section introduces OmniIndex's patented solution for regulated data by outlining how its innovative use of different technologies combine to provide a new powerful yet accessible solution for sensitive and confidential data storage, distribution, and analytics.

Significantly, while the result of OmniIndex's technology is new with innovations in a number of different areas, the core components are not new ideas. Indeed, at the core of the product is encryption.

This is one of the defining features of data security with Article 32 of the GDPR including it as an example of an appropriate technical measure.

Likewise encryption features prominently in the CCPA recommendations. It is listed both as an accepted standard of security in keeping with the Center for Internet Security's Critical Security Controls (the minimal level of security required in the CCPA), and as a recommendation in the Attorney General's '2016 Data Breach Report' following its investigation into good data management and security practices.

The type of encryption OmniIndex utilizes in its FHE blockchain is AES 256. This is a higher level of security than is currently required in order to be compliant with the outlined regulations and it is currently seen as 'virtually impenetrable using brute-force methods'.

With traditional encryption methods, a file is encrypted with an authorized key and then anyone with the corresponding key can decrypt the data file and return it to its original form. It is a widely available measure with a low-cost of implementation. What's more, because it is widely used there are a number of reliable and secure key management systems in place to ensure key security.

The OmniIndex uses the same concept of encryption, but adds additional benefits through a patented process. This process defines data objects while encrypting the data enabling computations to be performed on the data in its encrypted state.

For OmniIndex customers, this means being able to analyze encrypted data and gain the same results as if the data had been analyzed in a decrypted form. This is crucial because it means that at no stage of storage or transmission does the data risk violating the regulations with it always encrypted at rest and in transit.

Significantly, this encryption is not done by OmniIndex but privately by the organization with only them able to authorize and authenticate users. This means confidential data always remains secure with the confidentiality, integrity and availability of the data never compromised with regulatory compliance thus achieved.

In addition to being encrypted, The OmniIndex sandboxes all data so that each user has their own data bank.

This means that unlike with many traditional data storage systems, it is impossible to accidentally access data that you are not authorized to view with only data in that specific sandbox viewable to the one who has supplied the required credentials.

By storing the data in this manner of combined sandboxing and encryption, it is possible to ensure the ongoing confidentiality, integrity and availability of the data with the knowledge it is secure and private at all stages of use.

Furthermore, because the data is stored in a proof-of-stake blockchain, it is not located in a single place for a potential attacker to target. Instead, it has a peer-to-peer distribution method with it shared and stored across multiple servers with the data always encrypted and sandboxed.

In addition to the security benefit of this meaning there is no single place to attack, it also means that if one block was to go down due to an attack or database issue, the data would not be lost with the other authenticated holders of the information able to securely reshare the blocks again until the chain is once more complete.

As well as meaning the data is protected from loss in this way, it also ensures another part of the regulations are fulfilled with article 32 of the GDPR stating a need for “the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.”

As an example, with The OmniIndex a healthcare provider can encrypt their DICOM images, upload them to the blockchain, and then allow authenticated users with given secure credentials of an encryption key and username and password to view the data from anywhere and perform analytics on that encrypted data. The results of the analytics are the same as if the data had been in plaintext and include potential results such as data visualizations showing what types of scan have been performed by which machines. Insights from such analytics could be used in real-time to ensure efficient management of these expensive pieces of equipment with insights around device optimization facilitating rapid and cost efficient patient care.

Similarly, a healthcare provider could distribute sensitive health data across the world through the blockchain with the data encrypted at all times and only those authenticated to do so able to view it. As one specific example, this could enable patients to view their own personal health information and records remotely with complete security and privacy, thus enabling the data to be shared across multiple medical practices.

Finally, there is no need to build new datastores or migrate sensitive information as The OmniIndex is a simple plugin and will run safely and securely on any Cloud Infrastructure. What's more, the OmniIndex team are experienced leaders in big data and the onboarding process is designed to be straightforward for customers with one-to-one assistance provided.

What is important to point out, however, is that it is up to the customer to manage their encryption keys with this an important part of both data security and the regulations with reasonable security expected to be in place to protect and authenticate their use. OmniIndex do not hold these keys, with only the customer in charge of granting access to their encrypted data.

In summary, while the implementation of OmniIndex's patented FHE technology within the blockchain is unique, the technology at the core of The OmniIndex solution is pre-existing with the military grade encryption and blockchain technology already identified as respected and highlighted solutions for secure data management.

Significantly, what the platform offers is the ability for users to increase their data security and regulation compliance by enabling data to remain encrypted while it is stored, distributed, and analyzed.

OmniIndex

The data revolution is ongoing with new regulations being proposed, negotiated and introduced continually. However, at the heart of these regulations is a set of core principles focused on ensuring the decisions around how the data is used are lawful, and that the data is protected at all times to ensure its security, confidentiality and integrity is never compromised.

The OmniIndex offers a solution for this with its use of an FHE blockchain ensuring data is encrypted to the highest possible level at all stages of use - from storage, to distribution, to analytics.

When accompanied by secure and considered key management along with data protection officers and the legal collection and use of data, this solution offers a potential means for organizations to utilize their sensitive and confidential data compliantly while still distributing and analyzing it.

SOURCES

https://iclg.com/practice-areas/data-protection-laws-and-regulations/1-the-rapid-evolution-of-data-protection-laws

https://www.ibm.com/downloads/cas/OJDVQGRY

https://www.legislation.gov.uk/eur/2016/679/article/5

https://www.legislation.gov.uk/eur/2016/679/article/30

https://www.legislation.gov.uk/eur/2016/679/article/32

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-encryption

https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

https://omniindex-8753932.hs-sites.com/three-truths-data

OmniIndex

OmniIndex was established in 2020 with the sole purpose of building a suite of software tools to commercialize the application of fully searchable homomorphic encrypted datasets across a broad range of industries like healthcare, finance and insurance, and supply chain management.

For more information, visit our website https://www.omniindex.io where you can find other resources and our contact information.