



UNLOCKING INTELLIGENT INSIGHTS IN AN INCREASINGLY REGULATED WORLD.

A guide for DPOs and legal practitioners
looking to safeguard their organisation
against tomorrow's regulatory and
compliance challenges by harnessing
the power of AI.

What is this?

Keeping up with regulatory and compliance advancements is something every business needs to be aware of, especially as we enter another period of potential change. This guide explores the current state of regulatory play and identifies the key challenges UK businesses will face in the future. Alongside this, it presents a number of potential solutions to overcome these obstacles and alleviate the incoming pressure on compliance teams.

TOPICS EXAMINED INCLUDE:

- **What Brexit really means for UK businesses**
- **Developments in cybercrime**
- **The impact of the Schrems II case and the loss of Privacy Shield**
- **The increasing importance of data visibility**
- **How advancements in AI and machine learning are helping organisations to better manage regulatory developments**

Contents.

PROLOGUE 04

Executive Summary.

CHAPTER ONE 06

Introduction.

CHAPTER TWO 08

**The Challenges Ahead
for UK Businesses.**

CHAPTER THREE 14

**Under Pressure: The Impact on Ethics
and Compliance Teams.**

CHAPTER FOUR 20

**The Solution to Regulatory
Headaches.**

CHAPTER FIVE 25

**Intelligent Insights
into a Regulated World.**

PROLOGUE

Executive Summary.

Sometimes it seems that data underpins everything we do. That's because in many ways, it does. From influencing what we watch to determining whether we can see friends and family, data is the deciding factor. Its importance is only going to increase, with the world storing 200 zettabytes of data by 2025¹. And Gartner predicting that by 2023 more than 33%² of large organisations will have analysts practicing decision intelligence and decision modelling.

GDPR made everybody more aware of the importance of their personal data and a year of lockdowns has decimated many sectors and altered the way we work forever. As the realities of Brexit, and its increased regulatory requirements, return to top of mind for many business leaders, fresh challenges are arising for an already beleaguered business community.

This guide explores this current and future business landscape whilst uncovering the obstacles that could potentially impede economic recovery. From advancements in cybercrime to fresh regulatory headaches and the complexities of remote working, it will not only map the territory, but also serve as a guide to successful navigation via technological advancements in AI and machine learning.

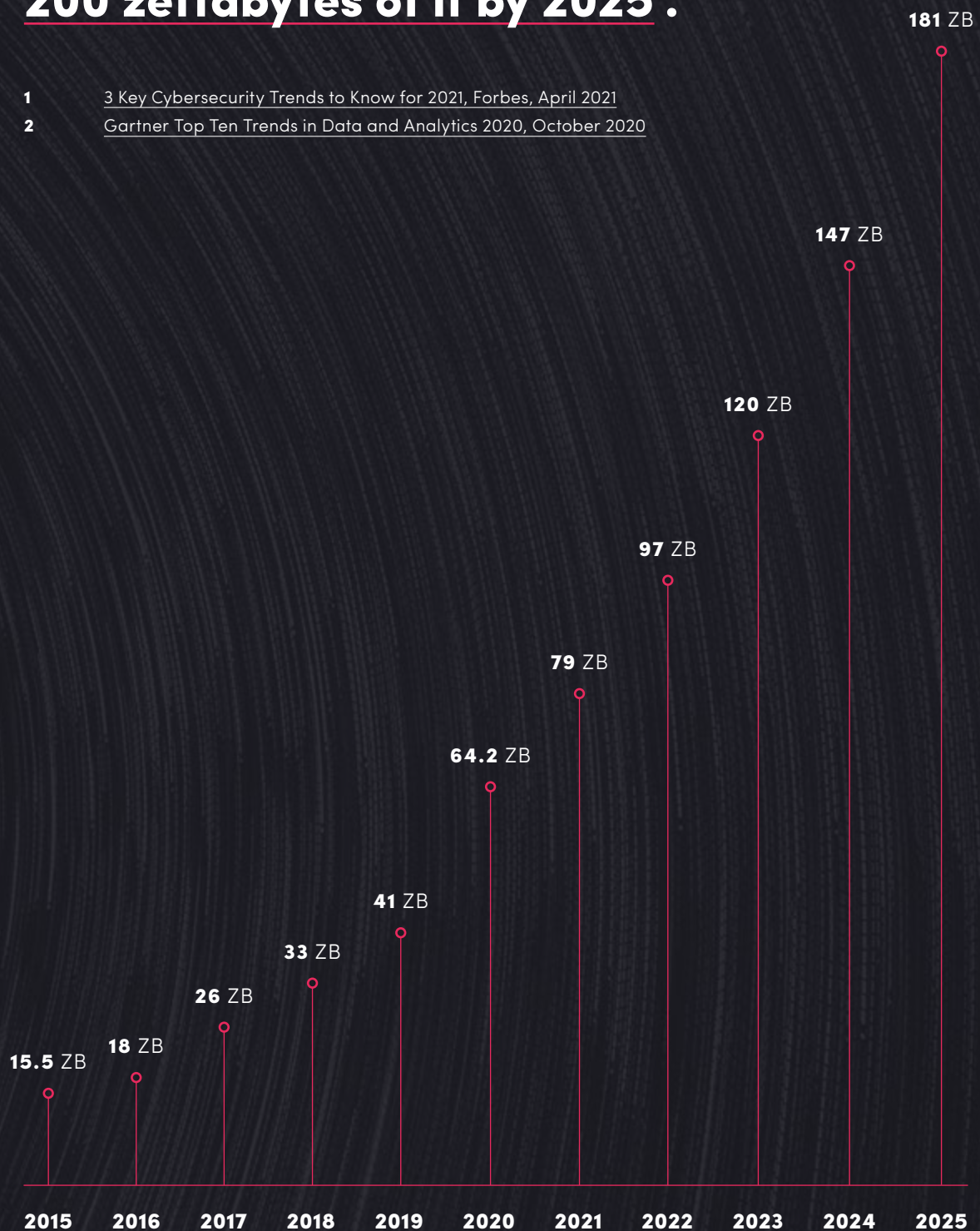
We hope you find it informative and enlightening, but also optimistic about the future. If you have any thoughts or questions regarding any of the topics, ideas, or solutions discussed, please contact us at enquiries@aiimi.com and we'll be happy to answer in any way we can.

**There's a new world arriving
and it's up to all of us to shape
and improve it.**

PROLOGUE CONTINUED

Data's importance is only going to increase, with the world storing 200 zettabytes of it by 2025¹.

- 1 [3 Key Cybersecurity Trends to Know for 2021, Forbes, April 2021](#)
- 2 [Gartner Top Ten Trends in Data and Analytics 2020, October 2020](#)



ABOVE Total data volume worldwide 2015-2025 | [Statista](#)

CHAPTER ONE

Introduction.

NEW BUSINESS LANDSCAPE, NEW BUSINESS CHALLENGES

One of the many things that the last year has brought to the forefront of public attention is the importance of data and how it can affect our lives — especially when it's organised and interpreted inefficiently. Hindsight obviously has a 20/20 vision, but better outcomes would surely have emerged from improved data-driven decisions. Governments and public health organisations were caught unawares by COVID-19 due to an inability to correctly interpret and act upon the data available.

Future pandemics are not an if, but a when and the vast amount of data accrued over the past 12 months is going to be integral in ensuring faster responses next time. What will be of equal importance to the amount of data is the way in which that data is stored, indexed, surfaced, contextualised, and ultimately, utilised. Because what we learn from the past can only help us improve the future when we comprehend it correctly and deploy it contextually.

These factors apply equally to businesses facing new regulatory challenges and the risks they can entail. Fortunately, rather than searching for answers, it's now possible to have relevant data appear in context to respond to these business requirements. That's because many businesses already have the information they need — they just don't know it. As our CEO, Steve Salvin, points out, "From our analysis, 73% of the documents created by companies have never been used since the day they were created. Companies are systematically rebuilding information that's already there, wasting valuable resources and time." Instead, the key obstacle businesses face is making sense of their existing data. Receiving these timely insights without the need for human prompting has the power to transform business performance.



CHAPTER ONE CONTINUED

“

**From our analysis,
75% of the documents
created by companies
have never been used
since the day they were
created. Companies
are systematically
rebuilding information
that's already there.**

STEVE SALVIN, CEO, AIIMI

After the deluge of pandemic-related information, rapid change and employee disruption, some challenges that were placed on the back burner are now heating up again. Regulation and compliance are perfect examples. And with Brexit now very much a reality, the implications for UK businesses are especially pertinent.

This guide draws out the pressing regulatory and legal challenges now being faced by businesses, along with the practical impacts on ethics and compliance teams. More importantly, it illustrates the tangible benefits being realised by businesses that adopt insight engines as a solution.

CHAPTER TWO

The Challenges Ahead for UK Businesses.

Businesses face an array of complex and time-consuming challenges in 2021 as they emerge from the focus of the pandemic.

According to a Government survey³, four in ten businesses (39%) and a quarter of charities (26%) faced cyber security breaches or attacks in the 12 months to March 2021. Whilst the number of businesses facing attacks is reportedly lower in 2021 than 2020, the survey highlights an emerging gap in preparedness for the future: fewer business deploying security monitoring tools, and just three in ten with business continuity plans in place for cybersecurity.

**Four in ten businesses (39%)
faced cyber security breaches
between March 2020-2021³.**

**Just three in ten organisations
have a business continuity plan
in place for cybersecurity³.**

³ Department for Digital, Culture, Media & Sport, Cyber Security Breaches Survey 2021

CHAPTER TWO CONTINUED

Overall, the UN has reported a 600% spike in cybercrime since the start of the pandemic and as a consequence spending on preventative measures by businesses has increased by 10%, according to well-known market analysis firm, Canalys.

One key area that organisations need to focus on improving is remote worker security, as a lax approach can facilitate highly-damaging ransomware attacks. Criminals spend weeks or even months identifying a company's defences and gaining access to their systems. This way, they can maximise the impact of their attack — by also gaining access to backup servers, for example. These multi-stage, or “slow and low” attacks, often begin by harnessing credentials stolen from staff members and can go unnoticed for weeks.

CHAPTER TWO CONTINUED

AI and machine learning are proving to be powerful weapons in this field via their predictive capabilities. By having access to a large number of refined data points, they're able to recognise anomalies and anticipate potential threats. Think of it like playing chess against hundreds of opponents thousands of times. Over time, strategies are recognised and it becomes easier to spot potential attacks and cut them off before they become lethal.

In the case of machine learning, stack trace analysis creates a record of what happens at different points in time. By analysing what happens at each stage, normal activity becomes clear and a reference model is created. In the case of a ransomware attack, changes in behaviour would be noticed and alerts would be triggered.

Alongside this, the ability to track and trace where information is stored allows businesses to ensure that sensitive data is stored in the correct secure environments. By performing a simple automated sweep, an insight engine can determine whether files contain sensitive information. It then flags any anomalies to the user, who can take the appropriate action and prevent the potential for a damaging breach.

Alongside external threats from criminals and internal user-generated errors, businesses must also contend with an ever-increasing number of regulatory requirements. Understanding these issues is critical to ensuring there are plans in place to address them, otherwise businesses will find themselves non-compliant and exposed to potential enforcement action and fines.

The ability to track and trace where information is stored allows businesses to ensure that sensitive data is stored in the correct secure environments.

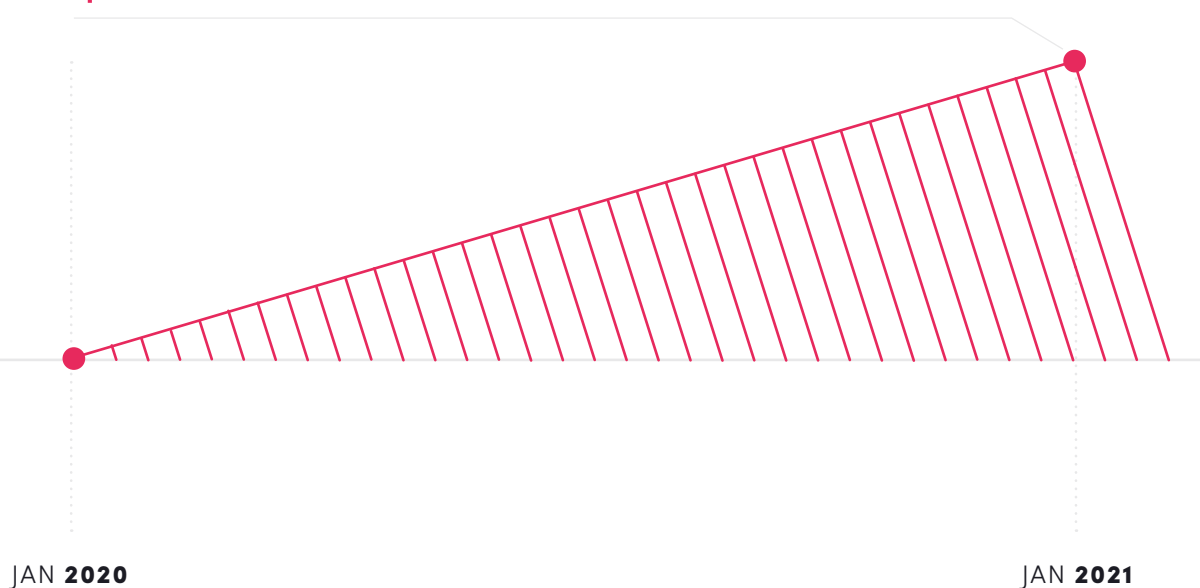
CHAPTER TWO CONTINUED

To take GDPR as an example, the first 18 months since it came into effect in May 2018 were extremely quiet. Where were all these big fines that everyone had been warned about? Things then began to ramp up considerably. In fact, according to research from DLA Piper, between January 26th 2020 and January 27th 2021:

- **GDPR fines rose 40%**
- **Penalties under the GDPR totalled \$191.5 million**
- **Data protection authorities recorded 121,165 data breach notifications (19% more than the previous 12-month period).**

What this implies is that it could be two years before Brexit-related punitive punishments start appearing. But businesses who don't start taking precautions now could find themselves on the wrong end of some hefty fines down the line. No one would like to end up in H&M's shoes who were hit with a \$41 million legal decision for monitoring several hundred employees and breaching the GDPR's principle of data minimisation — don't process personal information, particularly sensitive data about people's health and beliefs, unless you need to for a specific purpose.

Penalties under the GDPR totalled \$191.5 million.



CHAPTER TWO CONTINUED

Brexit — outside the EU but inside GDPR.

The UK's high data protection standards have just recently been formally recognised by the EU, allowing the continued free flow of personal data from the EEA to the UK. This is positive news for UK and EU businesses which will not be required to put in place an additional legal basis, such as Standard Contractual Clauses (SCCs), to transfer personal data between the UK and the European Economic Area (EEA), allowing data to flow as long as UK and EEA businesses are observing their respective data protection frameworks.

A key element to note about the adequacy decision is that transfers for the purposes of UK immigration control are excluded from the scope of the adequacy decision adopted under the GDPR. This is in order to reflect a recent judgment of the England and Wales Court of Appeal on the validity and interpretation of certain restrictions of data protection rights in this area. The Commission states that it will reassess the need for this exclusion once the situation has been remedied under UK law.

Furthermore, the decisions also include a 'sunset clause', meaning that they will automatically expire four years after their entry into force and will be reviewed before being renewed. The European Commission will also continue to monitor developments in the UK data protection regime very closely, and holds the power to amend, repeal or suspend the decisions if required.

The UK is now a Foreign Country.

The other direct impacts of Brexit are the extra border checks and paperwork. Both importers and exporters have already experienced a slowdown in freight across the EU/UK borders as the UK takes on *third-country* status in the eyes of the EU. UK businesses will also need to adapt to any new regulations that the UK and EU agree. For example, EU licensing, copyright, trademarks and patents, environmental standards and the transfer of data between the EU and UK.

CHAPTER TWO CONTINUED

Schrems II case — a defeat for the Privacy Shield.

To compound these challenges, a ruling by the Court of Justice for the European Union in July 2020 has created further issues. **The Schrems II case** struck down the Privacy Shield Framework. For businesses operating in the EU and the US, this removed the liability protection for vendors moving data out of the EU. For that reason, it's likely to have invalidated many existing client contracts. Businesses that operate in any capacity within the EU will now have no option but to conform to EU privacy standards.

Without the Privacy Shield Framework businesses that collect personal data from consumers — almost all businesses with a website or mobile app — cannot use legacy EU Standard Contract Clauses (SCCs) to protect themselves. The challenge now is to track down any end-user licenses, privacy policies or service-level agreements that include those SCCs and amend them as soon as possible. For most organisations, searching for the relevant clauses across a wide range of documentation will be a time-consuming exercise. Performing this activity manually will also drain key staff away from other compliance-related activities.

Privacy Shield 2 is not on the horizon.

Whilst a successor to the Privacy Shield Framework is possible, there's no certainty on when this is likely to emerge. In the interim, the number of requirements for businesses will no doubt continue to increase. This will translate into a fresh workload of new policies and policy updates, both large and small, for staff to manage. Businesses will need to roll out training and learning to ensure their staff not only comply with the new legislative environment, but are also able to navigate new working processes.

CHAPTER THREE

Under Pressure: The Impact on Ethics and Compliance Teams.

Much of the impact born from these regulatory and compliance challenges will fall heavily on ethics and compliance teams. As the individuals responsible for protecting their businesses, they'll take on the lion's share of the critical work necessary to respond to this new landscape.

THE ONLY CERTAINTY IS CHANGE

The nature of the new regulations and legal decisions mean that **few businesses will be able to avoid making changes**. Compounding the challenges outlined earlier, there are also likely to be internal change initiatives led by the strategic priorities of individual businesses. Many organisations placed major programmes and **infrastructure projects on hold last year** as the pandemic set in. Once restrictions lift, it's anticipated that many of these will be relaunched, creating new requirements around compliance in their wake.

The consequences of which mean continuing uncertainty for ethics and compliance officers. They'll need to juggle competing short- and long-term challenges as changes are introduced. This requires a delicate balancing act to continue providing good governance, ethics, compliance and regulatory risk management.

**Few businesses will be able
to avoid making changes.**

CHAPTER THREE CONTINUED

CHANGE LEADS TO INCREASED RISK

Making significant process and policy changes at any time always increases the level of risk within a business. However, alongside these shifts are the ongoing impacts of the pandemic on the workforce – extensive working from home, high levels of employee turnover, and increased use of contractors. With employees also potentially furloughed, disengaged or under limited supervision, risk exposure is approaching critical mass. Compliance teams are going to be stress-tested whilst stretched to full capacity. Errors are going to be inevitable, and fines could follow swiftly in their wake.

Most businesses are organised around different teams, each focused on delivering their own separate functions. But this structure also leads departments to store their data and content in silos; for example, only allowing fleet managers to view information within the fleet management system or supply chain teams only being given access to the asset management system. The experience of Aiimi from working with its clients is that this is the source of many issues. “Often, non-compliance occurs because one piece of information has fallen between the cracks. Information is simply not joined up,” explains Salvin.



CHAPTER THREE CONTINUED

“

One of Aiimi's findings is that often, non-compliance occurs because one piece of information has fallen between the cracks. Information is simply not joined up.


STEVE SALVIN

CHAPTER THREE CONTINUED

THE SECURITY OF EMPLOYEE AND CUSTOMER DATA

High-profile data breaches have made people realise the value of their own personal data. A McKinsey survey of 1,000 North American consumers found that 52% of consumers trust companies that do not ask for information not relevant to their product. This increased focus on data protection means they pay more attention to mistakes and errors. As a result, controls on sensitive data have taken on much greater significance. Because problems that occur with this data can be the fastest way to lose employees and customers.

With the vast amounts of data stored within a single enterprise, one of the imperatives for businesses is to fully understand the risks they're carrying with personal information, as well as intellectual property and sensitive data. What makes this even more challenging is the proliferation of data across network drives, file shares and cloud data stores. Businesses not only need a clear understanding of where data is stored across the organisation, but also what's contained within that data. Only with that knowledge can business leaders have assurance over the security that surrounds employee and customer data.



52% of consumers trust companies that do not ask for information not relevant to their product.

CHAPTER THREE CONTINUED

THE SECURITY OF EMPLOYEE AND CUSTOMER DATA

The **recent increase in data subject access requests** (DSARs) illustrates the shift in people's attitude towards their personal data. GDPR also introduced some changes that makes responding to them more challenging for businesses. For instance, organisations may no longer charge a fee, except in certain circumstances, and now have only 30 days to respond. Failure to respond to DSARs can leave organisations open to the higher level of administrative fines under the GDPR: €20 million or up to 4% of annual global turnover – whichever is greater.

Responding to DSARs is time consuming without the aid of a relevant technology solution. If a business were to accrue a backlog of requests, meeting the allocated response time manually would become extremely difficult. Especially if they were suffering from a lack of qualified staff capable of handling the workload.



Organisations now have only 30 days to respond.

Fines under the GDPR.

Up to 4% of annual global turnover.

**or
€20 million**

CHAPTER THREE CONTINUED

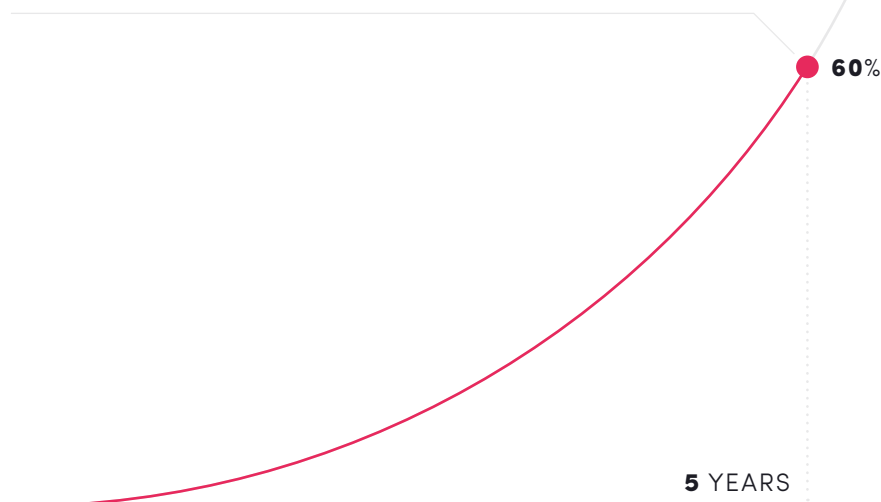
THE DATA SKILLS POOL IS TOO SHALLOW

It's clear that the challenges of regulatory pressures are going to place extreme pressure on compliance teams. This means that the demand for experienced staff with the right data and digital skills is going to accelerate in tandem. However, there's already a severe shortage of sufficiently skilled individuals in these sectors.

The **Learning & Work Institute** has recently highlighted the UK's digital skills shortage as "catastrophic". Its survey of over 1,000 businesses identified that 60% of employers believe their requirement for advanced digital skills will rise over the next five years. With this need unfulfilled, on top of last year's upheaval, compliance teams could reach breaking point. This increases the threat of compliance risk exponentially and will have a knock-on effect across other areas of the business.

How can compliance teams balance the intensified demand for specialist skills with a fractured work environment? The answer lies in advancements in AI and machine learning working in conjunction with employees to improve data management and highlight pertinent information. An area which the Aiimi Insight Engine is currently at the forefront of.

60% of employers believe their requirement for advanced digital skills will rise over the next five years.



CHAPTER FOUR

The Solution to Regulatory Headaches.

Most organisations digitise documentation, but they struggle to turn data into meaningful information. The reason is that technology solutions have too often focused on simply how to store the data rather than how to use it effectively. As a result, the opportunity to improve productivity and performance, reduce risk and makes things compliant comes from joining up the dots with information.

These regulatory changes call for a new strategy to allow businesses to resolve those challenges without it taking a toll on ethics and compliance teams.

INSIGHT ENGINES: INTELLIGENT IGNITION

Insight engines take a different approach to other information solutions. They allow businesses to generate insights from existing data wherever it's stored, rather than migrating it to a new platform. The software advancements powering this technology can discover both structured data and unstructured content whilst it remains in file shares, email servers, or data lakes. Not only this, but they can also surface this data at the right time and place. What this means is that users can become aware of information previously obscured from them. Unknown unknowns, if you will.

The role of the Insight Engine is firstly to raise awareness, by shining a light on data that's important to an organisation at that moment in time and to make it visible. Then it provides people with the tools to mitigate against the risk that poses. This allows businesses to preempt rather than react to these challenges. As Salvin puts it, "Essentially, you're now able to ask your information a question and get an answer back."

CHAPTER FOUR CONTINUED

“Essentially, you’re now able to ask your information a question and get an answer back.”

STEVE SALVIN

With the challenge of new regulations, insight engines make it possible to respond faster by accessing information dynamically. For example, to discover user licenses, agreements, and policies that relate to a particular area of regulation. Or to find documentation that contains information covered by export controls. A better understanding of existing information allows businesses to pinpoint where changes are necessary. With this knowledge, they can plan the most effective way to make updates.

Compliance teams can also gain insights into the level of risk within their business. Instead of searching for specific instances of non-compliance, visual dashboards can instantly provide the answers. An enterprise view shows a summary for the whole business, whilst also allowing inspection of individual documents. This enables compliance officers to focus on the source of problems and take action to correct them through training or support.

An additional way insight engines provide assistance is by facilitating the connection of people within an enterprise. Applying contextual tags to existing stores of data opens up the opportunity to discover all the people who’ve created or modified a document on a topic. With the capacity of compliance teams strained, this capability can help them to identify not only the individuals who have the most knowledge or interest within a certain subject, but also who’s interacted with any document throughout its lifecycle.

Automation can also support legal activities like eDiscovery by surfacing information for disclosure. With access to data and content across the business, all information related to a specific case or dispute is identified. To make this process more efficient, sensitive data can be automatically redacted before documents are disclosed.

CHAPTER FOUR CONTINUED

It's similar to the experience of walking into a library and knowing where to find the information you're looking for. It has its own classification system, so books go on a certain shelf in a certain order. There are also rules to take books out or return them. Most companies try to do that manually with their information management for processes and policies. But with people being people, they don't follow those rules. It's as if all the library books are thrown into a heap on the floor. The value that the Insight Engine can bring isn't only to put those books back on the shelf. But to allow people to search for particular words or phrases across the library.

Salvin describes the Insight Engine as adding "myriad other dimensions to let you consume the knowledge in a way that makes sense to you." Or, to put it another way, the future approach to business information can be thought of as like the experience of browsing a streaming service such as Netflix.

Netflix first presents viewers with a thumbnail image of each film's trailer, along with a description of the plot, the actors, year of release, rating, genre, and so on. It then also suggests similar films, highlights what other people have watched and provides recommendations based on what you've seen before. This all seems simple and obvious to us now, but it's actually incredibly subtle and smart. By presenting information in this way, viewers can assimilate contextual information at speed and more coherently, which leads to improved decision making.



CHAPTER FOUR CONTINUED

“The Aiimi Insight Engine adds a myriad of other dimensions to let you consume the knowledge in a way that makes sense to you.”

STEVE SALVIN

In much the same way, the Insight Engine allows businesses the opportunity to start visualising information in a way that’s meaningful to them. For example, when searching for an invoice, the thumbnails of other invoices from that supplier are immediately visible, or the purchase order related to that invoice can be viewed. Just as we now see Netflix’s way of displaying information as the obvious way to do it, we’ll soon feel the same way about how insight engines present information to us at work.

A NEW WAY TO SEE INFORMATION

The Insight Engine’s ability to find new relationships between data is the key to unlocking valuable information. That can be hard work though when the only tool available is a complex spreadsheet. However, the Aiimi Insight Engine allows the surfacing of relevant information at the right time and in the right context. This intelligent approach opens up a range of intuitive ways for ethics and compliance teams to analyse information.

In addition, interactive tools like animated graphs have the potential to provide immediate insights into vast and complex data sets. Visualisations that link documents to maps and site diagrams can show the location of problems or opportunities. Whilst voice control enables data interrogation to be performed at greater speed alongside other tasks.

Bringing together disparate sources of data in this way can be extremely powerful. Salvin highlights that “data and content are really one information landscape, so surfacing insights comes from being able to join them together.”

These applications provide businesses with a different way to interact with data. The ability to contextualise information moves us beyond a focus on big data. Instead, businesses are now able to make better use of their captured data and turn it into transformational insights.

CHAPTER FOUR CONTINUED

“

**Data and content
are one information
landscape, surfacing
insights comes from
being able to join
them together.**

STEVE SALVIN

CHAPTER FIVE

Intelligent Insights into a Regulated World.

In a world in which data-driven decisions have been shown to literally make the difference between life and death. It's now more important what we do with it, rather than simple accumulation for its own sake.

The digital data explosion has made information intangible — we no longer physically interact with our data. Previously, paper documents, locked filing cabinets, or even hard disks reminded us of the importance of what they contained. Today, everything exists in a digital aether and that can make us careless. Software platforms such as the Aiimi Insight Engine have the power to reconnect us to our data by presenting it to us in ways that better suits our cognitive abilities. Not only that, but by surfacing it contextually, we're reminded of its history, relevance, and ongoing importance.

Forward-thinking businesses are already realising the potential of machine learning, AI, and insight engines to handle repetitive, yet still sufficiently complex, tasks. The Aiimi Insight Engine isn't here to replace human workers, it's here to allow them to focus on the more business-critical aspects of their job. The future will still be human-made, just with assistance from our AI co-workers. Those who embrace this now will be the first to reap the rewards of the next IT era.

CHAPTER FIVE CONTINUED

**Book your demo of
the Aiimi Insight
Engine today and
discover how it
could transform
your business.**

BOOK NOW →



CHAPTER FIVE INTELLIGENT INSIGHTS INTO A REGULATED WORLD

Aiimi Ltd
100 Avebury Boulevard
Milton Keynes, United Kingdom
MK9 1FH
enquiries@aiimi.com
0123 456 7890