one connected community

Whitepaper

Tackle GDPR: OCC Findings 2018

The clock is ticking for GDPR (General Data Protection Regulation) compliance. There is mounting pressure to deliver a GDPR strategy that not only mitigates the risks of non-compliance, but balances the need for stand-out customer relationships and long-term business objectives.

Overview

To help insurers on their journey toward GDPR compliance, One Connected Community (OCC), Microsoft and Hitachi Solutions joined forces to host a group of senior insurance executives at London's Gherkin for a thought-provoking workshop. The conversation focused on exploring the practical steps that insurance businesses can take to achieve compliance and to leverage the many opportunities that the GDPR presents.

The insights, crowdsourced* directly from insurance professionals provide a benchmark for insurance businesses working toward GDPR deadline day, May 25, 2018.

The report highlights that, if managed well, GDPR can help inspire stronger customer relationships. But, to get there insurers must set a new standard for data privacy.

Getting your house in order

78%

...of our insurance businesses have conducted an information audit to map data flows

The looming GDPR deadline provides a catalyst for insurance businesses to get on top of their data, and subsequently leverage it to its best effect, across multiple business functions.

As Udo Pickartz, EU Head of Compliance, Starstone Insurance, puts it: "Many parts of the GDPR have been covered in previous data protection principles.

*About the research: *This research was developed by One Connected Community in partnership with Hitachi Solutions Europe between September 2017 and March 2018. Contributors include senior executives from: Wesleyan, Swiss Re, OBE, Enstar Group, Aspen Insurance Group, Canada Life, Hyperion Insurance Group, LV, Starstone Insurance, Munich Re, Brit Insurance, Covea Insurance. One Connected Community would like to thank all contributors for sharing their time and insights.*

"However, elements of the GDPR including increased levels of fines have stimulated a greater focus on better data management. It's an opportunity to make sure your organisation isn't tied up in knots by legacy. It's an opportunity to get control of what you have, which for many, until now, has been a very messy area."

In addition, Andy Gill, GDPR Programme Manager, Hitachi Solutions, notes that the cost of data storage is another catalyst for insurance businesses to conduct a data audit. He says: "Historically, the economics didn't make sense to tidy up your data. The cost of re-mapping data was much more expensive than simply retaining it indefinitely. But, accounting for the potential costs of GDPR non-compliance, the economics has flipped. This drives better retention policies, records management, information classification etc."

The challenge is now not the cost of data storage, but the risk of data storage. Given the data-acquisitive nature of the industry, retention and deletion of data is a particularly troublesome aspect of the GDPR.

The retention dilemma

Of all aspects of the GDPR, retention and deletion of data is perhaps the most complex for the insurance industry to navigate. Insurance businesses are data rich and many processes rely on the acquisition of data over time (and the subsequent intelligence that data provides).

As such, there is a reluctance to simply delete data. Instead, insurance businesses propose a multitude of strategies, systems and approaches to be compliant while retaining data where possible. Simply put, the overarching objectives of the business (growth and new policy acquisition) may well suffer if GDPR pulls the plug on an ocean of data that has accrued over time.

What to retain? What not to retain?

When tackling the retention dilemma, it's vital to have a thorough understanding of the importance of different data sets, for various business processes. For instance, key policy information may require a relatively lengthy retention period to allow for late reported claims.

As Adrian Dobrovicz, Business Architect, LV, puts it: "Different areas across the business have different demands on data. What you're doing on the front end in terms of retention, must match the business use further downstream."

28%

...of our insurance businesses have a process in place to dispose of personal data when it's no longer required or where an individual asks for it to be erased

Anonymisation

One approach to avoid deleting data is through anonymisation and pseudomisation, says Anwar Ahmed, Head Solutions Architect, Munich Re.

"Regarding retention, investing in anonymisation gives you a great alternative to deleting it. Data analysis, over time, becomes better and keeping data gives us more opportunity to draw insights from it. Considering this, moves to avoid deleting data are our best course of action."

Anonymisation is, of course, the process of turning data into a form that is not personally identifiable. But, given that an individual can be identified by a reference to an identifier such as an ID number, or location information, ensuring data is 100 percent anonymised is a tough task.

Anonymisation requires each insurance business to take a risk-based view on the extent to which anonymisation can reduce the compliance burden versus the risk that anonymisation is not 100 percent effective.

Legal basis

Tanya Jacobs, Group Risk Manager, Hyperion Group encourages an approach that emphasises consideration of the legal basis for the retention of data.

"Strategising around data retention requires a simple question: Is there a legal or regulatory reason for retaining data? To retain data the answer must demonstrate a business need and be in the best interest of the customer."

55%

...of our insurers have identified a lawful basis for processing data

Transparency

A successful response to GDPR is one that is regulation led, but creates commercial value too. A notable opportunity to create commercial value is to build customer trust. Being transparent around how you're using customer data will go a long way to building a trusting relationship.

Andy Gill, GDPR Programme Manager, Hitachi Solutions, explains how demonstrating customer-centric data management is a massive opportunity. He says: "Clear consent and privacy notices create a dialogue that stresses to the customer: 'this is your data, we're looking after it and we're doing an exceptional job of it.'"

It is this interaction that provides the opportunity to build trust. Unsurprisingly then, only:

11%

...of our insurers believe GDPR will have an adverse effect on their ability to market to customers

Conversely, greater transparency presents a huge opportunity to foster better quality relationships with customers.

Data subject rights

Despite the low historical volumes, it is important to consider the potential of a large surge of subject access requests, due to the publicity surrounding the GDPR.

"GDPR's publicity creates a 'shop window' for customers to exercise rights around their data. Should the business not have in place a process for dealing with such requests, there could be subsequent reputational damage for the business," says Amanda Hurst, Head of Compliance, Canada Life.

Such requests are particularly difficult to manage for insurance businesses with multiple legacy systems. If a business is seen as disorganised and unable to handle requests, claims management companies may take advantage of it.

"To mitigate against a vast number of data subject access requests, transparency is key," says Steve Jackson, Head of Financial Crime, Covea Insurance.

"Communication with customers must stress how good you are at managing their data. That way you can build confidence with your customers to ensure they don't flood you with subject access requests," he adds.

That said, the complexity of the insurance distribution model means data subject access requests are particularly tricky from a technical perspective. For instance, while most insurers can pull data subject information from their own systems, there is also an expectation that the data controller will also be able to extract that data from partners with whom the data is shared.

Demonstrating compliance

Above and beyond implementing GDPR compliant data management procedures, insurance businesses are obliged to document data processing, safeguards, policies and maintain their records as business processes evolve.

The maintenance of accurate records may add a significant resource burden, says Udo Pickartz, EU Head of Compliance, Starstone Insurance.

“You can do all the right things and put all steps in place to be GDPR compliant. But crucially, if you don’t have documented evidence to prove it, you may run into a problem with the regulator. A system of maintaining evidence is crucial for demonstrating ongoing compliance,” he adds

89%

...of our insurers have a process in place to detect and report a data breach

Stuart Riley, Group Compliance Director, Aspen Insurance Group, agrees that to maintain sufficient evidence of compliance is crucial. However, he argues that the infusing of a culture of privacy by design is the bigger challenge. He says: “Maintaining records of policies and procedures is one thing, but the challenge is around culture i.e. how many people actually follow those procedures.”

As a litmus test, insurance businesses should ask themselves: Would I pass the test if the regulator measured the practical implementation of our policies and procedures on a day-to-day basis?

Culture change

Getting your culture right is vital, says Andy Gill, GDPR Programme Manager, Hitachi Solutions.

“You can have the best systems, processes and will in the world, but the way people act must reflect that. It’s a journey towards educating businesses that data belongs to customers; it’s only to be stored if there is a legitimate interest to do so.

“From a regulatory standpoint, issues such as storage on personal devices and printing documents can be counter-compliant. However, changing those processes is no mean feat. It requires changing the very habits and beliefs that people have,” he adds

As testament to the difficulty of cultural change, only:

33%

...of our insurers are confident that their whole organisation is fully aware of the importance of better data management under GDPR

For Hyperion Group, one of the options is to lock down anything that isn’t connected to the network, says Group Risk Manager, Tanya Jacobs.

“A hard deadline for colleagues to transfer all their information onto the approved system may incentivise them to adapt new practices and hopefully cause less headaches in the long-run. The trick to changing habits is making the compliant route the path of least resistance.”

Additional approaches include, role-based permission, says Adrian Dobrovicz, Business Architect, LV.

“However, role-based permissions are complex to manage. For instance, internal team transfers will result in different access rights - the challenge is to facilitate changing permissions without it becoming a huge administrative burden,” he says.

Final Thoughts

Whether implementing new business processes, embedding technology or documenting your policies and procedures, it's important to maintain an effective balance. A balance that ensures compliance, but does so in a way that keeps the overarching business objectives front of mind.

GDPR is a broader governance issue, says Stuart Riley, Group Compliance Director, Aspen Insurance Group. "The danger is that we get to the end of May simply as a tick-box compliance exercise."

Success lies in recognising that compliance and delivering commercial growth are not mutually exclusive, but in fact go hand-in-hand. GDPR compliance must be delivered in a way that is coherent with the commercial model of the business.

This means setting a higher standard for customer privacy. Those who do so will become trusted custodians of personal data, resulting in richer, long-lasting customer relationships.

Infusing a culture of privacy by design is crucial. While cultural change is a difficult task, it is a necessary one that sets the standard for better data management and transparency; standards which customers increasingly expect from their insurance providers.

How Hitachi Solutions can give you the edge?

Are you struggling to manage complex and numerous legacy systems? Are you juggling data in order to piece together a fragmented view of your customer? Are your systems providing everything needed for explicit consent? Does your technology allow for subject access requests and seamless data portability?

Hitachi Solutions work within the insurance sector to find innovative and effective ways to unite complex silos of information. Hitachi Solutions enable GDPR compliance with a 360° view of the customer. Through uniting what is very often a compartmentalised structure, its systems work to eradicate inefficiency and ensure compliance. From policy admin to claims management, Hitachi Solutions work to improve processes, add value and build customer loyalty.

Contact Hitachi Solutions to find out more: www.hitachi-solutions.co.uk/contact-us/

Hitachi Solutions

Microsoft | Dynamics 365