REPRINT

R&C risk & compliance

AML COMPLIANCE – DATA PRIVACY CHALLENGES

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-SEP 2019 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

Acuris Risk Intelligence

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

ONE-ON-ONE INTERVIEW

AML COMPLIANCE – DATA PRIVACY CHALLENGES

Nick Parfitt
Head of Market Planning
Acuris Risk Intelligence
T: +44 (0)20 3741 1200
E: info@acuris.com

Nick Parfitt is responsible for determining Acuris Risk Intelligence's approach to the market and building subject-matter expertise. He has 18 years' experience in project and programme management, business process change and in implementing technology and business solutions at financial services, telecoms and public sector organisations. His experience in the financial crime sector spans seven years helping tier 1 financial institutions assess and improve AML, KYC and sanctions operations. Mr Parfitt has worked for several tier 1 banks in the UK and holds an MBA (Distinction) from Cardiff University, and a BA (Hons) in Biochemistry from Imperial College.

R&C: In your opinion, how has the regulatory environment governing anti-money laundering (AML) developed in recent years?

Parfitt: As new channels and means of value exchange become available, the regulatory environment continues to evolve and expand in response to new threats and challenges. We saw tax evasion become a predicate crime, which is controversial and arguably not an AML issue, but the use of cryptocurrencies and pre-paid cards certainly is. Cryptos, with their cutting-edge technology and plethora of new coin offerings, do present a significant challenge as regulations struggle to keep up with the pace of change. I think we are also seeing a global convergence of AML regulatory standards as jurisdictional 'arbitrage' is being eroded. This is particularly true around the traditional issues of secrecy and non-disclosure of ultimate beneficial ownership and registers.

R&C: Could you explain the correlation between AML legislation and evolving data protection issues?

Parfitt: The questions we often are asked around data protection and how it relates to the AML agenda and need for personal information, typically relate to a perception that because personal data is becoming more and more inviolate, it cannot be used for financial crime compliance purposes. This simply is not the case. As long as an organisation clearly documents the purpose for which the data is being used and adheres to its controls to ensure appropriate access – and other policies such as data retention periods – then there should be no conflict between the requirements of data privacy and AML data usage.

"As new channels and means of value exchange become available, the regulatory environment continues to evolve and expand in response to new threats and challenges."

Nick Parfitt, Acuris Risk Intelligence

R&C: How would you gauge the impact on AML compliance and data privacy of both the EU's Fourth Anti-Money Laundering Directive (4AMLD) and the General Data Protection Regulation

(GDPR)? What sanctions do businesses face in the event of non-compliance?

Parfitt: The application of GDPR to ensure compliance within organisations has been challenging. Organisations have had to clearly understand how, where and why data is obtained and used and how it flows, both internally and where it is shared with third parties. They have also needed to set policy statements and contractual obligations between parties. This has required significant organisational effort, especially to create the necessary legal statements, contracts and opinions. For AML compliance, where customer data is processed against watchlists via third parties and in multiple jurisdictions, this has caused significant 'drag' as organisations work to ensure compliance with the requirement for new contracts between parties. Failure is not an option given the size of the penalties: €20m or 2 percent of revenue, whichever is higher.

R&C: What do you believe are the main data privacy issues and challenges that businesses need to overcome to ensure AML compliance?

Parfitt: Possibly the biggest impact and trend is towards jurisdictions not allowing customer data to be processed outside of that country. This introduces significant costs and complexity as infrastructure needs to be replicated and cases cannot be managed in offshore or near-shore centres. Beyond this challenge, in our opinion, it is more about the documentation of the data and processes and ensuring data is only being used for AML purposes. Note too, that certain sensitive data elements, such as religious and sexual orientation, should be carefully evaluated as to their appropriateness for AML purposes.

R&C: Given the large quantities of high-value data they often hold, how should businesses go about designing and implementing systems and controls that can effectively manage the cyber security and data breach risks they face?

Parfitt: This is no easy task and should be an ever-evolving process that is regularly reviewed. However, an organisation should start by scoping out the data it holds and assessing risk in terms of loss and the material impact to the organisation. If your customers' home and account information is compromised, how would this impact your reputation and future earnings? What would be the cost of remediation? Also, the organisation should take a holistic approach to its cyber security risks and exposures. What is the point of having multi-million dollar hardened networks and firewalls if the CEO's home network is weak or unsafe public

Wi-Fi access is regularly used to access sensitive commercial information? Equally, if someone posing as a lunch delivery service can gain access to critical floors, then this makes a mockery of physical security.

R&C: How would you characterise the importance of tools such as encryption and containerisation in addressing data privacy requirements? What additional methods are available to help businesses ensure AML compliance and protect data?

Parfitt: Clearly, the use of encryption to secure sensitive data is fundamental to adding an additional layer of privacy and can be applied 'at rest'. This means that if a database is hacked, its information should in theory be protected as it is not readily viewable without a private 'key'. However, it is likely that a dedicated hacker could find tools available to crack even the 'strongest' hashing technology, especially if quantum computing becomes a reality. More forward-looking organisations not only employ the latest security tools and techniques, but also ensure that staff are constantly reminded of their information security responsibilities. They use simulations to try and trap employees into clicking on bogus links that look legitimate – we see this as being particularly effective. Companies should also look to monitor the dark, or non-indexed, web for their company and employee data as a way to provide not only a 'baseline' of potential vulnerability, but also as an early warning system for potential breaches.

R&C: What essential advice would you offer to businesses on creating a strategy which ensures ongoing compliance with an evolving AML and data privacy paradigm?

Parfitt: Firstly, risk-assess the data you are using and holding and the purpose of its use, and document and agree the assumptions and flows with the business and its data protection officer. Secondly, fully assess who is processing or controlling the data and for what purposes, and look at the security controls and policies relating to your overall information security policy and procedures, particularly staff training. Finally, hold simulation exercises and business impact assessments for breach scenarios that include key stakeholders to determine the short-, medium- and long-term implications. R&C