Securys®

ENTERPRISE INSIGHTS

KYC, AML and data privacy – is your business getting the basics wrong?

The consequences of not getting up to speed on data security can be crippling for a small business, both financially and from a customer retention perspective.

It can be hard to know where to start navigating the waters of Know Your Customer (KYC) and Anti-Money Laundering (AML) checks when it comes to data privacy. But it is essential to get the basics right.

Data protection legislation is principles-based and so gives you some autonomy in terms of being able to make decisions about how exactly you manage information best. This allows organisations of all different shapes and sizes to operate within the law and do the best thing for their customers without running to unnecessary expense or additional resources.

How do you collect your data?

It's all too easy to just think about consent when you consider data privacy.

A lot of checks are conducted to comply with specific AML legislation and this processing is necessary. What's important to bear in mind – particularly in a GDPR context – is that those legal obligations apply, or pertain only to EU or member state law, or in the UK context to UK law.

AML = Anti-Money Laundering

KYC = Know Your Customer

KYC checks are conducted in the interests of protecting your organisation.

KYC checks are conducted in the interests of protecting your organisation and should demonstrate that those interests are sufficient relative to the risk of intrusion. This means you should conduct an assessment to demonstrate to any regulator that you've given due care and attention, talked about the risks and put adequate measures in place. Not being able to demonstrate this makes you much less likely to be able to meet your obligations.

Are you minimising the data you collect and keep?

We hear reports of people doing KYC checks involving social media scraping in order to make an evaluation about their customers' perceived wealth and assets. But it's not within the purview of an organisation to go around hoovering up people's social media feeds. This is not proportionate processing for the types of checks that are taking place. Seeing whether someone's got an extra fancy car, or is taking lots of holidays, in order to question the source of their income, is not ok.

How much information do you need to collect and what information do you need to record and keep? If you're working with a third party, what information does that third party report back to you? And what information do you need in order to form a judgement about someone? Are you asking them to report that they've passed a credit check or are you asking for a detailed 35-page Experian report? It's important to stay on the right side of minimisation by collecting only the information that's necessary to fulfil the purpose of confirming the checks.

Doing the right thing in terms of your organisational process should end up with you doing the right thing from a data protection perspective.

It can be tempting to use a blanket approach to evidence collection but this is a risky strategy. Instead, tailor your approach according to the risk that applies, not just from a data protection perspective but also from a generalised AML perspective.

The two things go hand in hand. Doing the right thing in terms of your organisational process should end up with you doing the right thing from a data protection perspective. Acting responsibly with regard to people's information is just an extension of acting responsibly around your interactions with them. You build trust by acting appropriately and – crucially – you lose trust by failing to do this.

If you ask a customer for a copy of their passport are you currently asking for an unredacted copy of their passport? Or are you simply verifying their identity and then redacting the record that you keep? What you really need is a record that you have verified their identity. There are plenty of high-end technological ways of redacting evidence but a thick black pen or a scanned photocopy with pieces cut out works just as well. Holding on to the original evidence can leave the data wide open to misuse, and leave you open to breaches.

Are you being clear in your communication?

Transparency is a key principle of data protection. It's the law to make it clear to people what you're doing with their information. Particularly in the context of AML and KYC, it's important to inform people that you're collecting information from other sources. The same applies to notifying people of breaches – in fact, failure to do so leaves you open to fines, not to mention bad press. This is why being transparent at all times will help prevent you from falling foul of GDPR – and other – regulations.

Who's looking after your data?

Not everyone in your organisation needs to have access to everything. Sometimes you just need to know that someone has completed a check rather than be able to see the details of the check. Dedicated training for the people who have access to the most sensitive material is also a good idea. A very good guiding principle is to manage the transition from desirability to necessity. Ask yourself, "Do I need this piece of information to do my job?" and "Have I always had access to this piece of information, even though I didn't need to have access to it?" The money laundering reporting officer at the estate agent might need to see your passport, your estate agent does not.

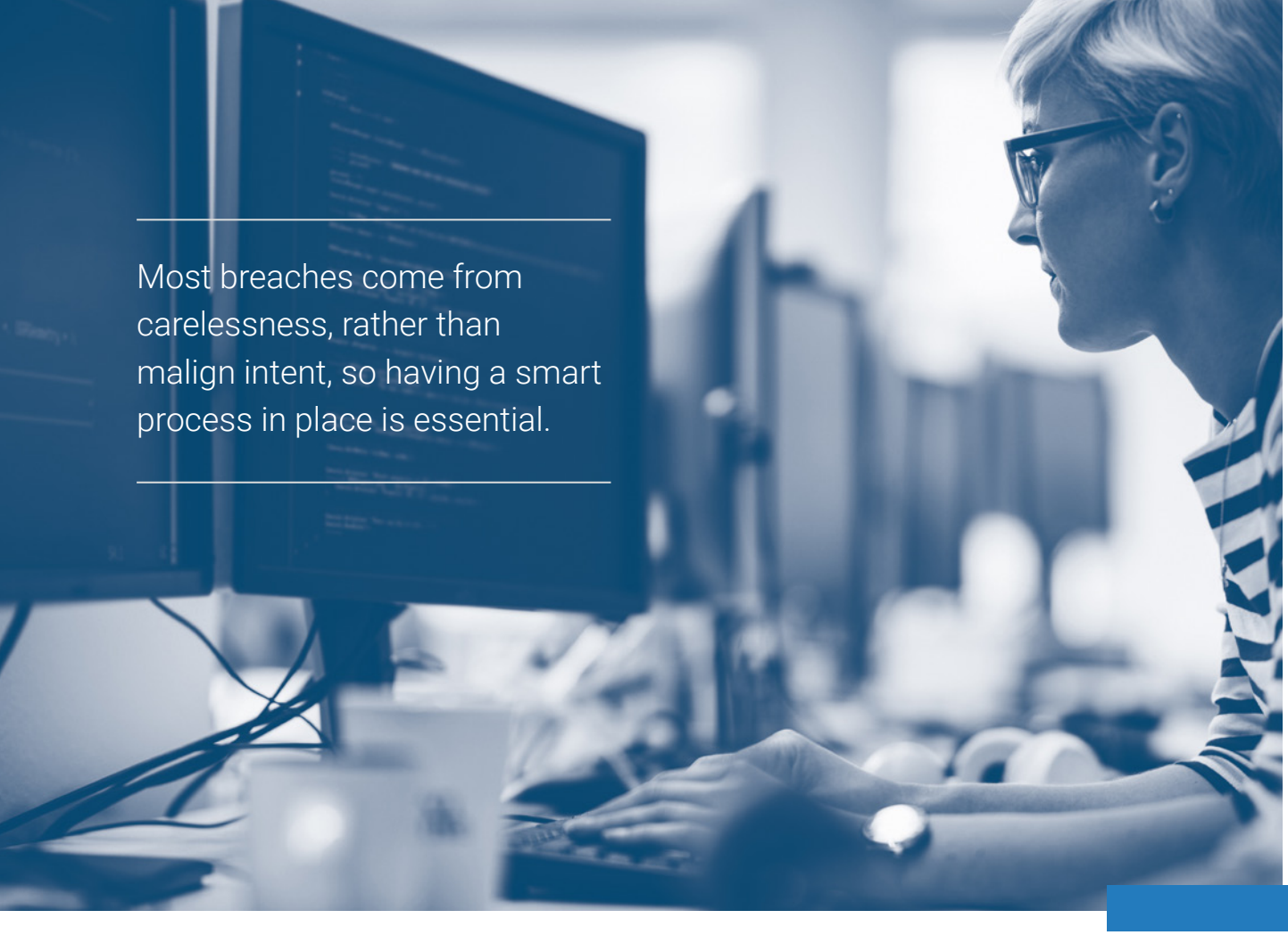
Do you have good processes in place?

A lot of good data security is simply about having smart processes. Do you have a process in your organisation that can be reviewed on a regular basis? Again, you could take a technological approach which automates the deletion of information every quarter or you could take a lo-fi approach and simply review your records three or four

Watch our webinar

To watch our webinar on KYC, AML and data privacy, visit:

www.securys.co.uk/webinar-kyc-aml-and-data-privacy



Most breaches come from carelessness, rather than malign intent, so having a smart process in place is essential.

times a year. Most breaches come from carelessness, rather than malign intent, so having a smart process in place is essential and this might mean getting the right experts on board to help you.

Who are your third parties?

What care have you taken around outsourcing? If you rely on agencies or service providers, which many of us do, what steps have you taken to give yourself and that by extension, your customers, the assurance that they are going to handle your information in the right way? This might entail some form of assessment or evaluation – asking them for asking them to demonstrate their own credentials, testing to make sure that they understand the principles as well as you do both from a privacy perspective also from an information security perspective.

Where information is crossing international borders or being sought from countries outside the European Union, you will also need to demonstrate that you have considered the risks around that transfer of information.

Most customer service comes back to building trust and demonstrating best practice is a crucial part of building trust.

Are you treating your customers as customers, not criminals?

The fundamental point is that KYC isn't an excuse to treat your customer like a criminal. If you always take care to empower the customer, then you'll naturally ensure that your employees recognise that it's in everybody's interests for you to make use of data in this particular area. Most customer service comes back to building trust and demonstrating best practice is a crucial part of building trust. Being able to balance this with staying on the right side of the regulations may be a challenge but it is one everybody should be able to achieve.

About Securys

Securys is a specialist data privacy consultancy with a difference. We're not a law firm, but we employ lawyers. We're not a cybersecurity business but our staff qualifications include CISSP and CISA. We're not selling a one-size-fits-all tech product, but we've built proprietary tools and techniques that work with the class-leading GRC products to simplify and streamline the hardest tasks in assuring privacy.

We're corporate members of the IAPP, and all our consultants are required to obtain one or more IAPP certifications. We're ISO 27001-certified and have a comprehensive set of policies and frameworks to help our clients achieve and maintain certification. Above all, our relentless focus is on practical operational delivery of effective data privacy for all your stakeholders.

Securys®
Privacy Made Practical®

161-165 Farringdon Road
London
EC1R 3AL

T 0800 193 8700
E info@securys.co.uk
W www.securys.co.uk

securys-limited
@SecurysUK

UK0022/0322