Data protection and cyber security in a post-GDPR landscape

#KingstonIsWithYou

Foreword

Countless companies and organisations worked hard – and hired hard – to prepare for GDPR. Perhaps yours was one of them. Yet the ever-evolving nature of cyber threats means you cannot afford to stop and catch your breath. Compliance with GDPR is not a box-ticking exercise, but a framework through which to judge your ongoing data protection and cyber security efforts. There's no room for complacency.

In this short eBook, we pool the knowledge of some of the UK's most experienced commentators in cyber security to discuss how data protection has changed since the introduction of GDPR. We also cover how companies are educating their employees on the need for compliance and discuss how IT departments and tech providers can better secure IT infrastructure and educate end-users on emerging security challenges.

Contributors

This short eBook has been compiled by five experts in data protection and cyber security.

Rob Allen
@Rob_A_kingston

Rob is the Director of Marketing & Technical Services at Kingston Technology, and has been with the company since 1996. In his role, Rob is responsible for overseeing PR, Social Media, Channel Marketing with Digital Marketing Media and Creative for all Kingston brands and products.

Tara Taubman-Bassirian
@clarinette02

Tara goes by many titles: lawyer, advocate, mediator, researcher, consultant, speaker and writer. With incredible expertise in areas like privacy, intellectual property and data protection, she has made a name for herself in several areas of the world, most notably the UK, France and the US.

Rafael Bloom
@rafibloom73

Rafael is the Director of Salvatore ltd. In this role he helps companies to manage the strategic, commercial and procedural challenges and opportunities created by technological and regulatory change.

Miriam Brown
@Kingston_MBrown

B2B Strategic Marketing Manager at Kingston Technology, and has been with the company since 1997. In her role, Miriam is responsible for the marketing strategy, content and campaigns for all Kingston B2B products.

Sally Eaves
@sallyeaves

Prof. Sally Eaves has been described as the 'torchbearer for ethical tech'. She brings a depth of experience from Chief Executive Officer and Chief Technology Officer roles, as a Professor in Emergent Technologies and as a Global Strategic Advisor. Sally is an award-winning international keynote speaker, author, researcher and influencer sharing original and authentic thought leadership.

Table of contents

Section 1 – How has data protection changed since GDPR?

Companies have come a long way. In the last two years, legal teams have expanded, the recruitment of Data Protection Officers has skyrocketed[1] and consultation with external data privacy counsels has grown. The completion of data protection impact assessments (DPIAs) is now familiar to thousands of organisations.

But there is a long way to go.

One of the biggest challenges with GDPR is that you cannot take your eye off the ball. In most organisations almost any member of staff, at any time, could contravene the rules. The problem is magnified in sectors where the labour force is stretched or there's a high degree of autonomy – such as healthcare, education and law. In law, for example, many solicitors will think nothing of exchanging sensitive case details via a simple email attachment. Health professionals will exchange patient data or the results of an MRI scan from unsecured email addresses. In high-stress organisations all it takes is a little extra pressure on the to-do list for compliance to go out of the window. Productivity – it would seem – trumps protocol.

This must change.

Then there is the issue of awareness in the charity sector. Too often charities seem to think they are exempt from GDPR. Even when they do understand that GDPR applies to every private, public and third sector organisation, they are – perhaps understandably – reluctant to divert money away from their cause to invest in data protection.
That's noble but also naive. The potential fines for contravening GDPR dwarf the probable IT spend.

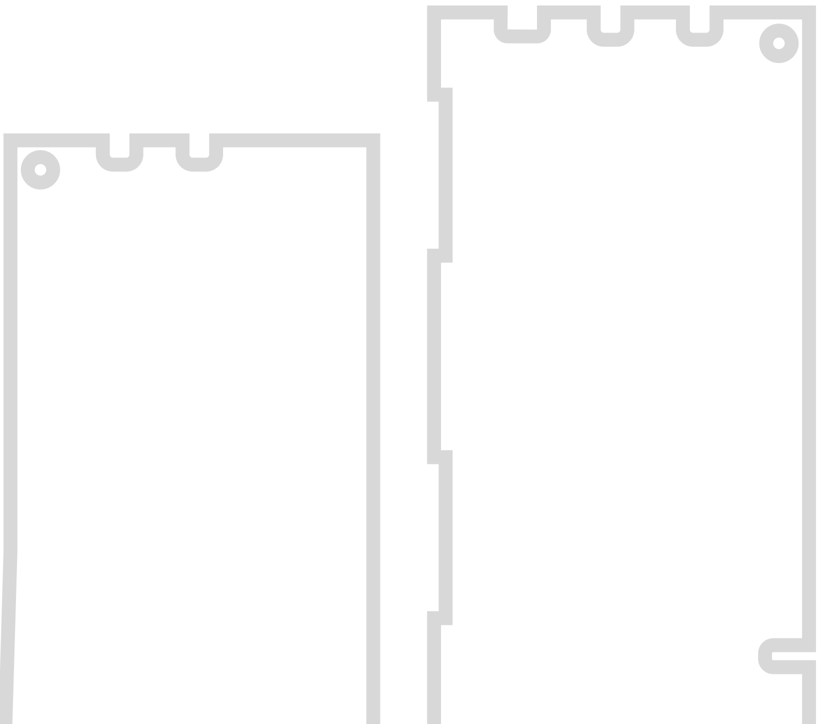
Since 2016 the demand for Data Protection Officers (DPOs) has skyrocketed and risen over 700%.

Tara Taubman-Bassirian
@clarinette02

GDPR, Data Protection
& IP Consultant

"Many third sector organisations say: 'GDPR doesn't apply to us, we're just a charity.' Even on website compliance I try to tell them it's not about the data that you want collecting, it's about the third party that you are allowing to get access to your visitors' data."

[1] Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [accessed 26.11.19]



How has data protection changed since GDPR?

Data minimisation is an encouraging trend

We live in an era of egregious data collection. "The Big Four" (Google, Apple, Facebook and Amazon) hold huge amounts of customer data. The assumption might be for other organisations to mimic The Big Four and collect as much data as possible. Yet the more data you carry, the more risk you expose yourself to. One of the most positive trends seen since the introduction of GDPR is a rebellion against excessive data collection. Smart companies employ an ethos of data minimisation: if you don't need it, don't collect it.

Tara Taubman-Bassirian
@clarinette02

**GDPR, Data Protection
& IP Consultant**

"Data minimisation is probably one of the best principals of GDPR. Any creation of a database means creating risk."

Rob Allen
@Rob_A_kingston

**Director of Marketing & Technical Services,
Kingston Technology**

"We have strict data deletion rules. Yes, business-critical data must be stored correctly. But for everything else? After a year it's gone. What's the point in holding it?"

The benefits extend beyond limiting risk. Take marketing, for example. If your marketing database is unhygienic, you may be holding obsolete data. When your database runs into the tens of thousands of people, and you conduct frequent email marketing campaigns, the costs add up. It skews your campaign performance stats too.

Data minimisation applies to physical data too. Be careful what you print off (such as scans of customer passports); be careful what you write down (such as account passwords). And when you do need to hold a physical copy of something, store it securely. That mountain of paperwork on your desk may look imposing. But secure it is not.

Rafael Bloom
@rafibloom73

**Director,
Salvatore Ltd**

"We are witnessing a completely different way of thinking about the interface between technology and what a business is actually doing. That level of digital maturity within business leadership needed to happen desperately."

Impact of exposure:
from the C-suite to the consumer

Data protection as a regulatory concept has been around for decades. But the large fines handed out thus far to companies including Google[1], British Airways and the Marriott hotel chain[2] – and the media coverage they generated – has bought GDPR to the attention of the C-suite. This has caused a trickle-down effect.

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways
   www.varonis.com/blog/gdpr-effect-review/ [accessed 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go?
   www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [accessed 26.11.19]

How has data protection changed since GDPR?

Continued...

Another driving force behind the adoption of strong data protection is collaborative business. Large businesses now perform extensive due diligence on the integrity of a potential supplier's data security because they don't want to be liable for data breaches by association.

There is also a flipside to the enhanced commercial awareness of GDPR: consumers are more aware of their data rights. And they know that if a company loses control over their data – note: there doesn't necessarily have to be a breach – they are entitled to compensation. Businesses must stay focused.

Sally Eaves
@sallyeaves

CEO and Director,
Sally Eaves Consultancy

"Data protection has become a business imperative where trust can be won or lost."

Staff training: two words capable of inducing eye rolls among your workforce.

More reason to make sure your training is engaging. An educated workforce is less likely to contravene good practice on data protection. And if there is a data breach, the Information Commissioner's Office (ICO) will look on you more favourably in their judgement, if you can prove that you have made efforts to train your staff on data security.

Rafael Bloom
@rafibloom73

**Director,
Salvatore**

"I like to think of data as a supply chain item, where its provenance and its entire lifecycle needs to have appropriate governance. It's all well and good getting your team in a room for half an hour and telling them what to do, please don't shred stuff, please have a decent password. Sure, you've lowered the risk to the organisation. But later, really, is there a material difference apart from that initial small impact that you kind of forced on people? No."

However, in April 2019, Digital Minister Margot James suggested that three in ten UK organisations have trained staff to deal with cyberthreats[1]. It's time to take training seriously.

It's about engendering culture, not tick box training

Training is about affecting genuine behavioural and cultural change, not about box-ticking. It's easy to purchase an online training package with some easy questions on data protection that anyone can answer correctly. But is that really going to help to protect your organisation?

Good data protection behaviours have two founding ingredients. Firstly, training that's smart, engaging and geared towards the unique challenges of your organisation. Secondly, realising that GDPR is a profound question of workplace culture that impacts all employees daily. It's about doing the right things with data, right the way through the organisation. Take HR for example. Think of all the personal candidate details that are just sitting on email servers.
Data protection is everyone's responsibility.

1. Intelligent CISO: One year on, what has been the impact of GDPR on data security? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [accessed 26.11.19]

How are organisations educating their employees?

There's a person behind the data

In the first section we noted that consumers are becoming more aware about their data rights. A good way to position data protection training is to help your staff make the connection that there's always a person behind the data. Ask your employees to think about every organisation that they have given data to and they realise that data protection is about personal privacy.

Have a contingency plan

Sally Eaves
@sallyeaves

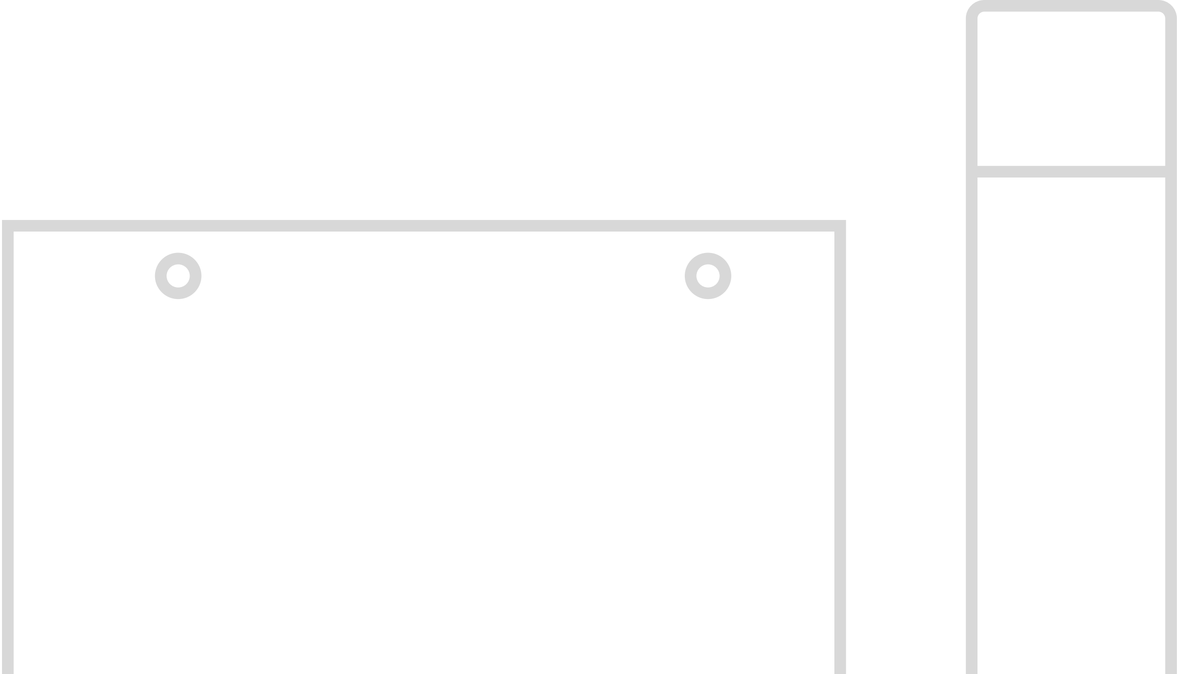
"Ongoing education for employees about data security and privacy is a business imperative. This must not be a one-off, once a year, training session, but rather a proactive, interactive and engaging experience so it is part of the everyday work experience. Employees must be involved in the dialogue about what we want to mitigate, manage and defend."

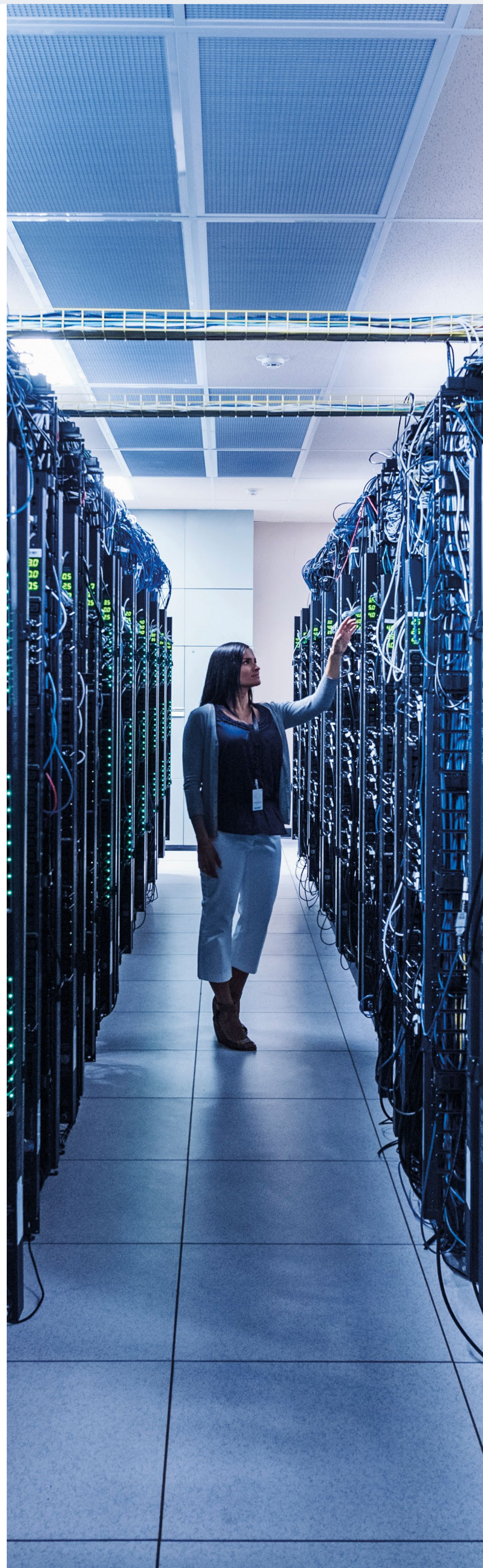
Miriam Brown
@Kingston_MBrown

"I think it's interesting during training when you say to people: 'what if it was your data?' If my bank manager was working from home on his laptop, and had sensitive information on that laptop, I would want it to be on an encrypted drive."

Rob Allen
@Rob_A_kingston

"Treat data as if it's your own."





Section 3 – Can IT departments better secure devices?

Remote working is the new normal

Your staff likely access their working world from several different devices – including personal devices that can easily be left on a train or lost in a taxi. Your challenge is to find a way to help your staff work efficiently without leaving yourself open to security risks and data breaches. All it takes is one person to bring your data protection efforts crashing down.

Sally Eaves
@sallyeaves

CEO and Director,
Sally Eaves Consultancy

"Data needs to be protected in transit, at rest and in use – it is critical to have an all-encompassing security, recovery and data erasure plan to cover across all of these contexts. Drawing attention to risk areas that are often underrated is particularly important, for example unencrypted USBs, using email for sending unencrypted attachments and web browser features exposing sensitive user data. With so many devices connected and working patterns evolving, it is critical to ensure that data stored on a mobile phone is as secure as data stored on a company server."

Two-factor authentication

For the average organisation, by far the best and easiest thing that you can do is to protect your network perimeter – and that really can be as simple as the use of password managers and two-factor authentication. A good example of two-factor authentication is when a user is prompted to supply a password on a laptop as well as a passcode that is sent to their mobile phone once a password has been successfully provided.

VPNs and encrypted SSDs/USBs

VPNs are increasingly popular with SMEs. They are particularly salient for staff who are accessing business data over public WIFI networks. But businesses must be careful not to overestimate the abilities of VPNs. They are part of, rather than the whole solution. Too often businesses deploy VPNs, only for remote workers to use notebooks or laptops without any hardware encryption. Nearly everybody stores files on their laptop. What happens if that device is hacked, lost or stolen? Encrypted USBs and SSDs are only marginally more expensive than the standard versions. Deploying encrypted USBs and equipping your notebooks with hardware encrypted SSDs goes a long, long way to resolving the challenges of remote working. And if a device is lost or stolen, you can be confident no one will have access to the encrypted files. You can even remotely destroy lost USBs.

"I once met a cyber security expert who attempted to persuade the CEO of a company to adopt two-factor authentication, only to be met with resistance: 'No, we are not doing it, it's a pain, it's an extra step, I don't want it.' Soon after they were the victim of a £40,000 fraud."

Rafael Bloom
@rafibloom73

Director, Salvatore Ltd

"Ultimately the best method to enhance security awareness is to open up conversations with employees to find strategies that are both secure and productive."

Rob Allen
@Rob_A_kingston

Director of Marketing & Technical Services, Kingston Technology

Can IT departments better secure devices?

Private servers and MSPs

Increasing numbers of large organisations are making the step up to having their own on-site servers again. That means they have full control over their server estate, with nothing stored in the publicly accessible cloud. Then there's hybrid server solutions where non-sensitive data remains in the cloud, but personal data stays on-site. For SMEs and organisations in the third sector, it may be too costly to have your own server. And that's where managed service providers and virtual private servers come in. It enhances the focus on security, without dramatically inflating your operational costs.

Auto-flagging of expiring data

One of the tenets of GDPR is the need to delete old data. Certain types of personal data, for example, must not be held for longer than seven years. What if you were automatically prompted when data was about to 'expire'? With the right database, it would be easy for your IT team to create an action that sent an auto-generated email to the DPO when you were approaching a data retention cut-off.

Work with the right vendors

When it comes to IT security, there are countless manufacturers and vendors. Do your research. It's all about having a system in place that comes from a trusted provider with specific expertise in enabling organisations within your industry or sector. Ensure that the vendor(s) you choose, not only have the technology, but also understand the adoption challenges when it comes to data security.

TLC for the DPO

Since 2016 the demand for Data Protection Officers has skyrocketed, rising over 700%.[1] There are now over 500,000 DPOs in employment across Europe – that's six times more than what was forecast back in 2017.[2] And yet the importance of the DPO's role is often overlooked and trivialised.

A DPO requires full visibility into your company's security and data privacy landscape. It's a full-time job. Yet in some organisations 'DPO' is simply a label allocated to the member of staff who best understands technology. They are responsible for their entire company's data privacy, all while performing the regular duties of their day job.

The reality is that there needs to be a range of professional services and tools available to support this new breed of DPO. Even if you do have a full-time DPO, data security moves fast and there will always be challenges that require a second opinion. Working with an external consultancy or counsel on data security can go a long way, but first you must have things as shipshape as possible internally.

Clarity, contingency and cohesion

Your IT infrastructure is only as strong as its weakest element. That's why for any new addition to your IT ecosystem, your tech provider should provide full clarity on the potential security threats and clear advice on how to use your new product securely.

Tara Taubman-Bassirian
@clarinette02

GDPR, Data Protection & IP Consultant

"I try to explain to people who install CCTV cameras everywhere that it is not necessarily security, because often they're installed without a password. So, you can just log onto a website, sit and watch. It's actually telling your robber:
'come and check when I'm not there!"

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [accessed 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [accessed 26.11.19]

How can tech providers improve processes and understanding?

There's the contingency issue. What happens when a product reaches the end of its lifespan or needs updating? Tech providers should provide contingency advice on their products inadvertently compromising the data it holds or exposing the security of your wider IT ecosystem. Take an MRI scanner, for example. It might come with a four-terabyte encrypted SSD for storing patient images. But what happens when that storage runs out?

Tech providers and organisations themselves must also facilitate an environment of digital cohesion and data cohesion – both within the organisation and when working with external suppliers and partners. That's especially crucial for multi-faceted, multi-departmental and multi-location organisations such as the NHS.

Miriam Brown
@Kingston_MBrown

B2B Strategic Marketing Manager at Kingston Technology

"We've sold a lot of products into the NHS - but there are definite differences from one trust to the next, when we ask what data protection policies and protocols they have in place."

Horizon-scanning

Tech moves fast, sometimes outpacing security. With emerging technologies – such as payment through facial recognition in China – it's sometimes the case that organisations race to get the technology out there before considering the potential security and data protection implications. The widespread availability of 5G networks is just a year or two away, where edge computing and distributed data silos will become a reality. Tech providers must be able to help organisations safely benefit from emerging technologies without compromising their own data integrity or IT security.

Sally Eaves
@sallyeaves

CEO and Director, Sally Eaves Consultancy

"I believe we will begin to see a change in GDPR away from reducing the pains of implementation, to focusing on optimising the gains, such as enhanced IT processes, backup and recovery, and improved security, and using these as a point of differentiation in relation to industry peers."

Summary

GDPR has changed business for the better, bringing data privacy and network security to the attention of the C-suite and consumers alike. Compliance, however, requires constant attention to data security – day in, day out – throughout your workforce. The ever-evolving nature of technology and cyber-threats means that good security infrastructure and good training – backed up by good consultative support on technology and data privacy – is all but business critical. Reminding staff that there's always a person behind the data can go a long way to embedding a culture of data protection within your workforce. And cultural change is far more effective than box-ticking training exercises.

About Kingston

With 32 years of experience, Kingston has the knowledge to identify and resolve your remote working challenges – making it easy for your workforce to work securely from anywhere, without compromising your organisation.

#KingstonIsWithYou