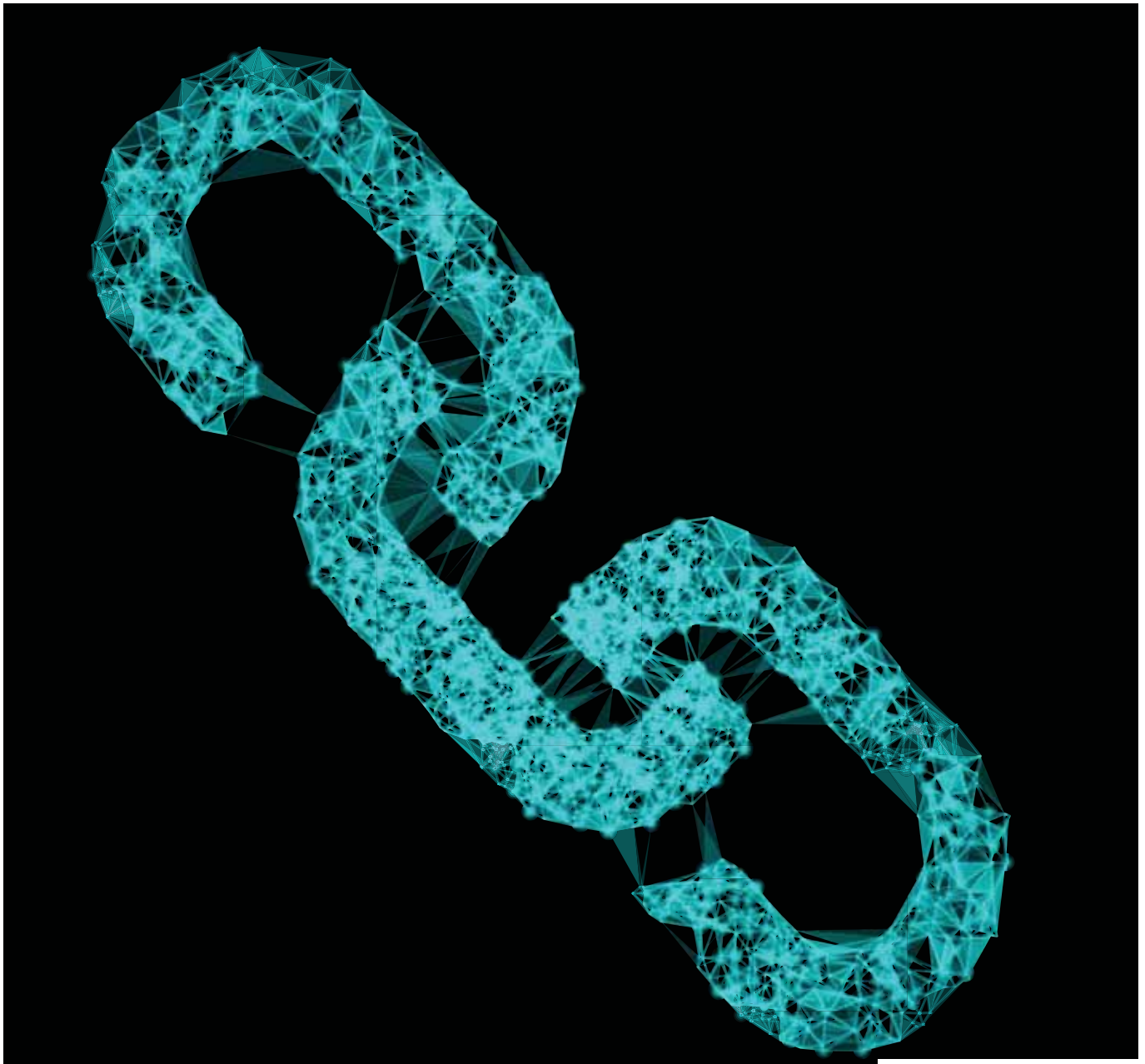
NewStatesman

Empowering services with smart data

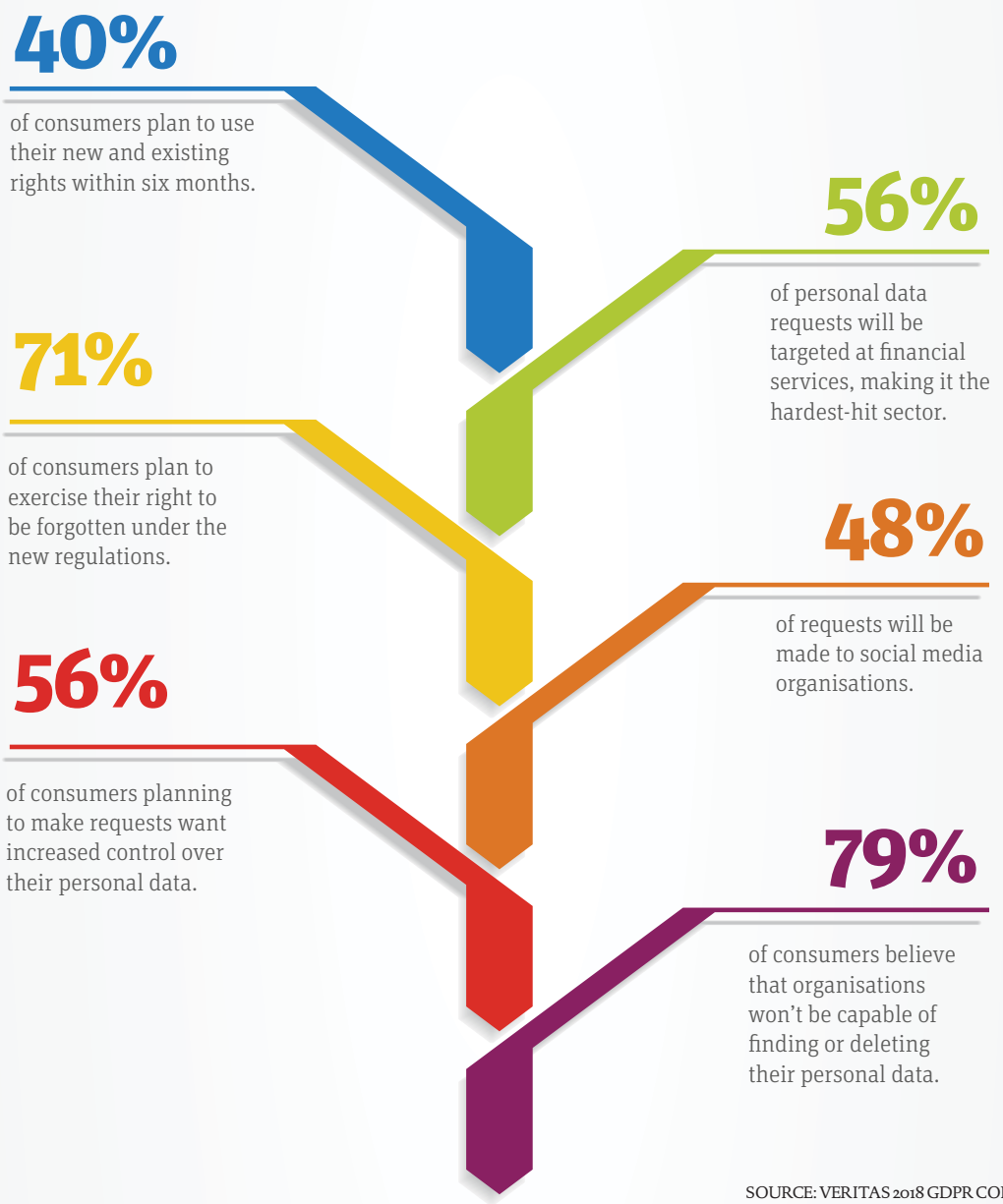
Realising the potential of data in the public sector



Sponsored by VERITAS

BY THE NUMBERS

How will GDPR change consumer behaviour?



SOURCE: VERITAS 2018 GDPR CONSUMER RESEARCH

NewStatesman
Standard House
12-13 Essex Street
London WC2R 3AA
Tel 020 7936 6400
Subscription inquiries:
Stephen Brasher
sbrasher@newstatesman.co.uk
0800 731 8496

Special Projects Editor
Will Dunn

Special Projects Writers
Rohan Banerjee
Augusta Riddy

Design and Production
Leon Parks

Cover image
Shutterstock/enzozo

Commercial Director
Peter Coombs
+44 (0)20 3096 2268

Account Director
Justin Payne
+44 0207 406 6530

The paper in this magazine originates from timber that is sourced from sustainable forests, responsibly managed to strict environmental, social and economic standards. The manufacturing mills have both FSC and PEFC certification and also ISO9001 and ISO14001 accreditation.

First published as a supplement to the *New Statesman* of 17 August 2018.

This supplement and other policy reports can be downloaded from the NS website at: newstatesman.com/page/supplements

SHUTTERSTOCK/KHVOST

The future of data is bright, as long as it is safe

Only when the risks are taken seriously will the benefits of data be reaped, warns Jos Creese, chief executive of Creese Consulting and former chief information officer at Hampshire County Council

With all the recent focus on GDPR compliance up to the 25th May deadline, it would be easy to lose sight of the bigger picture; the need for better management of personal data. In general, we've all become a bit complacent about our personal data. We enjoy the benefits that come with a willingness to share data, from more personalised services to instant access to an abundance of resources on our smartphones, but personal data abuse dangers are growing for business, government, individuals, and communities.

It's not just GDPR that has changed behaviour and attitudes. A flurry of recent information breaches and data scandals unsurprisingly meant that many organisations are now focusing on building (or rebuilding) a reputation for taking data handling more seriously. Indeed, the biggest social network firms are now vying for top position on data integrity and public data protection.

It's also not just about protecting our personal identity, privacy and assets. In politics and business, cyber risk has crept up the agenda, often becoming the single biggest threat to business continuity or competitive success. A serious data breach is more than a potential fine; it can undermine trust and reputation.

So while regulatory compliance is important, there is more at stake in protecting privacy. It would be easy to assume we don't need to worry because GDPR will protect us all, yet many companies are still collecting unnecessary personal data (such as when we connect to public Wi-Fi) and, despite GDPR, some are still selling our data or sending us unsolicited emails based on old marketing.

For GDPR to really work, it needs to permeate public awareness; that requires us all to recognise the risks as well as power of personal data. Data abusers play on our naivety, greed, and lack of digital literacy, and attacks are becoming more sophisticated. Often they link easily accessed personal data with real-life activities, using multiple channels – mobile phone hacking is growing faster than email phishing. Therefore, cyber awareness needs to be a part of core learning in schools, and a prerequisite for employment.

As we move towards artificial intelligence, robotics and the internet of things, it's easy to lose sight of growing public concerns around personal data. Governments may resist regulation, but it is as essential as environmental health controls to food preparation and sales.

GDPR, although important, is therefore only a part and a start. The public and private sectors must act now to develop strong information governance practices, and deploy the tools that allow individuals to be in control of their personal information. Otherwise UK digital development will be patchy and risky.

Post-Brexit, a key competitive advantage will be digital security. The UK could become the place to do electronic business, with high standards of digital service integrity and control, coupled with UK innovation and research. We have a strong UK tech sector, and we are building a global reputation for digital services. Exploiting these opportunities will depend on high levels of maturity in our use and management of data – particularly personal data.

GDPR is just part of the data solution

GDPR and the future of public sector data

Veritas and the *New Statesman* hosted a round table to discuss how public service providers can move past fear to embrace data and its boundless opportunities

On Tuesday 22nd May, three days before the much-discussed 25th May deadline for enacting GDPR, the *New Statesman* and Veritas gathered a group of MPs, civil servants and tech experts to discuss the future of data in the public sector and beyond.

GDPR is the General Data Protection Regulation, a piece of EU regulation aimed at encouraging the safe handling of personal data, and effective sharing of data. Failure to comply could have serious consequences; in the case of a severe data security breach, a fine of four per cent of annual turnover could be applied.

The impending deadline seemed to cause widespread panic amongst the public and private sector, an obvious sign of which was a flood of emails from various mailing lists asking people to "opt in", and recommit their permission to be contacted.

The *New Statesman* chair opened the discussion by reminding attendees that after the deadline, the compliance efforts wouldn't suddenly stop; business leaders will continue working out how to leverage data to make public services more effective and efficient. Viewing GDPR as a threat or extra administrative burden would be a missed opportunity, especially in the public sector where data has the ability to be transformative.

Vicky Ford MP, co-chair of the APPG on Internet, Communications and Technology, was invited to make some opening remarks. A former MEP, she came to the table with "a very long history of GDPR legislation, having seen a lot of its work as it went through the

THE PHOTO TEAM

European Parliament".

"The first thing I want to say is that we have to remember that big data and the ability to analyse it has got huge benefits for society," she began. Sharing it is important, she argued, if it's done correctly. "We need to get the right balance between being able to protect personal data but also ensure that we can have those benefits for society, particularly where data research fuses with medical research."

Speaking in her capacity as an MP on the Science and Technology Select Committee, she reported that when Elizabeth Denham, Information Commissioner at the Information Commissioner's Office (ICO), appeared before the committee "she described GDPR as not a single point in time; it'll be an issue that continues to evolve". GDPR is not "perfect", Ford argued; it is still developing.

Chi Onwurah, Shadow Minister for Industrial Strategy and co-chair of the APPG on Internet, Communications and Technology, followed Ford and offered some initial thoughts of her own. She said the influx of pre-GDPR emails showed "the power of regulation to focus the mind. For someone who has championed data rights since entering parliament in 2010, I'm really pleased to see data protection being taken seriously." However, she was critical of GDPR – "in my view the regulations are about seven years out of date" – arguing that it still doesn't enshrine data rights in an age of rapidly advancing technology. "I have asked the government to set out a framework for data rights for UK citizens and this is not it … Labour is planning a bill of digital rights, which will provide strong and easily understood protections for citizens."

She agreed with Ford that "the better use of data" would "make public services better," but warned that progress "comes with responsibilities to respect individual rights."

The chair then opened up the discussion to the rest of the table. Simon Holmyard, senior public sector sales director at Veritas, called GDPR "a good starting position to have a house cleaning exercise. Once you've got a good set of data, you can use it without fear of doing damage".

William O'Brien, senior manager of technical sales for northern regions at Veritas, concurred that GDPR was a "wonderful occasion for us to change our culture and behaviour towards how we manage and treat data."

The chair was keen to get the attendees' views on whether GDPR would scare companies away from working creatively with their data, or if they would use it to explore new options.

There was still a lack of clarity over accountability, argued Eleonora Harwich, head of digital and tech innovation at Reform, which could be making companies cautious. "Let's just suppose that there is a legal gateway to share data between the Department for Education and the NHS. Who's accountable for that data?"

Head of land transport security for rail strategy and security at the Department for Transport, Hannah Tooze, wondered whether "some good practice examples, as opposed to horror stories where something's gone wrong, might be helpful to build that confidence" amongst organisations.

"I think it would be really useful to have safe spaces or clearing houses where you could play and put bits of data together, but where the individual had control," replied John Paul Danon, sales director at the Council Advertising Network.

In terms of transparency when it comes to people's data, will there ever be a world where it can be explained how

"GDPR shows the power of regulation to focus minds"

an algorithm came to its conclusion, the chair asked. For example, if an individual applies for a loan online, and they are rejected without any human input, could the reasoning behind that decision be explained?

Onwurah asserted that there was an important distinction to be made; "it's not possible to explain how an algorithm works to lay people, nor should it be, but it is possible to understand how it works."

The Science and Technology Committee had discussed legality around algorithms, and therefore the possible need to "disclose how they were driving their conclusions," Ford reported. She said the Committee came to the conclusion that a good starting point was "if something is illegal in the offline world it should be equally illegal in the online world". "If you've got an algorithmic bias that says 'women are being shown lower-paid jobs than men [when they search online]', then that should be equally illegal."

The discussion moved on to personalising services with data sets; was this likely to happen any time soon? Aron Cheung, a researcher at the Institute for Government, confirmed that "people in senior management teams in public sector organisations do recognise data-driven changes that can deliver operational benefits to their organisation." He said that a lot of these changes are "also the changes that are needed to become GDPR-compliant", so GDPR was speeding up this process.

"I don't think the majority of people use data as well as they possibly could," said Danon, but he agreed that GDPR could act as a catalyst for exploring improvements. "If you have GDPR as an environmental sanitiser for all your plans going forward [then] everything you build will be built with that trust."

He claimed that among the public there was a level of "paranoia" about the use of personal data, and that the "education piece [of GDPR] has to happen as well as the compliance, so that people are easily able to see what's happened and when with their data."

O'Brien argued that "there needs to be some playground, this middle area where data can go and it has the right to be used legitimately" to encourage innovation in public sector data usage without fear of severe consequences. "At the moment accountability is holding everything back."

In the public sector, said Tooze, caution is prevailing. "At the moment we are quite compliance focused, so it's seen more as a risk that an opportunity … [but] information security isn't a new issue for government and all civil servants have mandatory information security training." Some of the issues raised by GDPR, she argued, "will be less new to government than they are to some areas of the private sector".

"I think it's a culture change," said Harwich. "You have to take everyone with you in an organisation." In a more developed data future, she argued, "data would follow people rather than the set activities. If I had a data trail on my phone then I can decide when I receive secondary care if I pass on my electronic health record, so then you would actually get effective direct consent all the time."

When it comes to health data, replied Danon, its potential to improve services could be demonstrated by presenting a common frustration, and showing how data could help to fix it. "The thing to do is start gaining GP-led consent from individual people to put initially very small numbers in and then demonstrate the value of that."

Concluding the discussion, O'Brien told the attendees that it was not just a matter of legislating and then leaving organisations to get on with it: "There is a responsibility to enable the communication of [GDPR] and the adoption of it."

As a company, Veritas is committed to supporting businesses to keep their data safe, and to understand GDPR and be compliant. Beyond that, it is actively supporting the public sector to explore the possibilities of data usage, creating smarter and better services for tomorrow's users.

Data solutions for Dorset Police

Dorset Police was struggling to manage its data, costing it valuable resources. Veritas was able to support the organisation to fix the problem

Dorset County comprises one million residents and more than 11m tourists a year, on 1,000 square miles of land. Policing a county that is 90 per cent rural is a significant challenge; the jurisdiction also includes an airport and multiple sea ports.

Compounding the challenge is data. "A change in our processes as an organisation related to a newly imposed records system," explains Adrian Stephenson, Infrastructure and Service Delivery Manager for Dorset Police. "[This] meant that suddenly there was a dramatic increase in the volume of data backup required. We went from three to four terabytes to 20 terabytes, just for our live system."

Dorset Police stores and handles a number of different types of data, including SQL and Oracle databases, VMware servers, and unstructured data files, and the sudden increase was costing Stephenson's team up to two hours a day trying to fix backup errors.

The existing infrastructure wasn't up to the job. "It hadn't been set with the new data volumes and goals," Stephenson says. "We needed a big boost in performance to make the original backup process reliable."

There was no extra budget available as the escalation in data was unplanned but the safety of the data was of the utmost importance to Stephenson's team. "We need to have absolute confidence in our disaster recovery systems."

Previously Dorset Police had been using Veritas NetBackup software and it had invested heavily in the initial system so was keen to see a significant improvement by upgrading. The organisation is now using a NetBackup 5230 Appliance which retains data at each of their sites, and the team then offloads monthly backups to tape for long-term retention.

The transition has been a success. "The Veritas NetBackup Appliances have helped us improve backup performance even as our data volumes increased by 500 per cent," says Stephenson. "They have already proven more reliable and stable than our previous solution."

His team has saved 60-80 hours a month, and the shift onto the new systems is expected to save £16,000 a year, meeting the tight budget requirements. "We now have 60 days of data on the Veritas NetBackup Appliances," Stephenson says. "We can retrieve data fast, resolve most requests instantly, and our deduplication ratio has also improved from 90 per cent to an impressive 95 per cent."

The switch has saved the team 60-80 hours a month

Delivering solutions like this strikes at the heart of what Veritas is trying to achieve in the public sector. Dorset Police, as a result of shifts in UK policing strategy, is now working in alliance with Devon and Cornwall Police, and the data handling systems provided by Veritas are expected to support this development. "More and more we'll be sharing back office systems and services between the two Forces," explains Stephenson. "It may be that we extend the use of Veritas NetBackup Appliances to include Devon and Cornwall Police. It would certainly make sense financially, deliver economies of scale, and simplify processes."

How do you protect something you can't see?

Your company holds petabytes of data, across multiple business units and countless systems. As much as 54% of this data is unmonitored and potentially risky. But now under GDPR, if a customer asks to see their data, you will need to respond – are you confident you could do that?

Veritas can help you locate and classify your unstructured data. Because you can't comply until you know what you're holding.

Take the first step today with our GDPR Risk Analyzer tool: veritas.com/gdpr

VERITAS™

The truth in information.