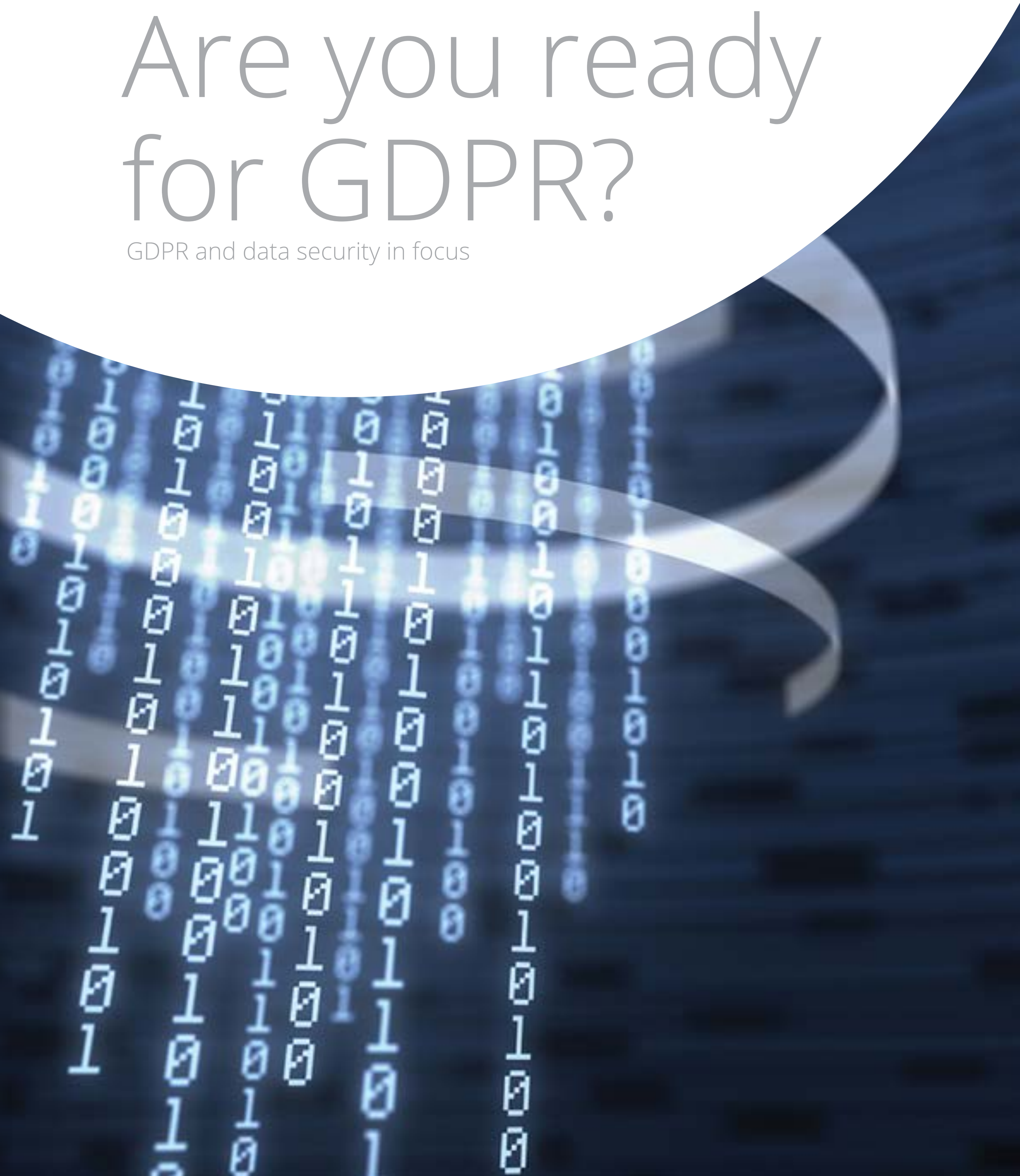
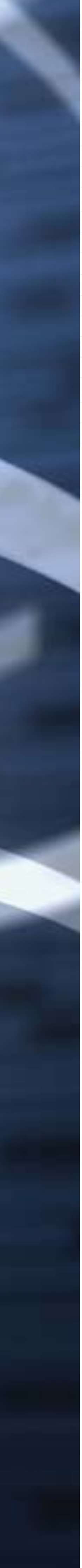
Avatu **datasecurity in review** white paper

avatu

Are you ready for GDPR?

GDPR and data security in focus





The Information Commissioner Elizabeth Denham has told businesses there's no time to delay in preparing for 'the biggest change to data protection law for a generation'. ✓ It's a complicated and far-reaching piece of legislation which poses both a threat and a challenge for many organisations. There is much you can do, however… but time is also running out.

The **General Data Protection Regulation (GDPR)** is changing the way organisations – both large and small - need to look after the personal and sensitive information they hold. And there's now less than a year to get it right.

When the GDPR rules were added to British law and the UK was given two years to get prepared before penalties began, some organisations realised the dawn of a new era had arrived. It was time to get serious about looking after their own business information and their customers' personal data.

Others thought: (a) GDPR didn't concern them, (b) the EU regulation could be repealed before it became actively enforced, or at least soon afterwards, or (c) they'd sort it out later.

Some were not even aware that the GDPR existed.

Unfortunately, for these organisations, the message is now a tough one.

- If you do business in the UK, or the wider EU, and you keep personal data (anything from IP addresses to bank details), it does affect you
- The British government hasn't repealed it and isn't likely to any day soon (it has one or two more pressing things on its mind)
- Time is running out. The deadline to have your compliant data protection policies and practices in place is less than a year away (May 2018). If you don't, you could be running the risk of the enormous penalties and perhaps the ignominy of being one of the first to fall foul of the new rules, which is why it's important to act now.

Renewed focus

Whilst the GDPR has been introduced to better protect EU citizens' data - and its implementation may disrupt the way many organisations operate - it should actually be considered good for business.

- **GDPR will help you manage risk effectively**, understand security dangers and protect your brand.
- **Companies should solve data security issues by approaching them from a business point of view**. The introduction of the GDPR has provided organisations with an opportunity (if not a wake-up call) to take full control of their data and re-evaluate security systems that are no longer suitable.
- **Many companies are looking at it as a prompt** to look at their data security as a whole.

20 million reasons to get it right

Organisations who collect or handle EU citizen records should be aware of a couple of headline items.

- Firstly, organisations who intentionally or negligently break the rules may be liable for fines of up to €20m or 4% of annual turnover, whichever is greater
- Secondly, organisations must notify a breach to their supervisory authority (which in the UK is the Information Commissioner's Office, the ICO) within 72 hours of its discovery.

Therefore, it is critical – because of these increased sanctions – that key stakeholders within the business fully understand the final legislative text.

The Information Commissioner Elizabeth Denham said recently that we stand on the edge of a new frontier due to the dominance and continued growth in the digital economy and the introduction of the GDPR.

Fortunately, however, there is a lot which organisations can do to reduce the risk, improve their data security and be GDPR compliant by the May 2018 deadline... but it has to be done now.

> GDPR will help you manage risk effectively, understand security dangers and protect your brand.

GDPR: everything UK organisations need to know in 60 seconds

Here’s a quick rundown of what it means to business:

Times are changing for data protection and security. The new **General Data Protection Regulation** - which come into effect in **May 2018** - increases privacy and gives new, far-reaching powers to regulators when it comes to a data breach.

DEFINES A DATA BREACH AS...
A ‘personal data breach’ is a “breach of security leading to the accidental or unlawful; destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.”

BIG FINES of up to 4% of annual global turnover or €20 million, whichever greater

DATA BREACHES
must be reported within 72 hours of its discovery. New reporting obligations apply to the data regulator AND, in some circumstances, the people who’s personal data is lost

The definition of PERSONAL DATA is wider and covers more issues

ORGANISATIONS NEED TO HAVE MORE CONTROL OVER THE PERSONAL DATA THEY HOLD. Organisations need a sound risk-based approach and a privacy strategy. Privacy risk impact assessment will be expected where privacy risks are high.

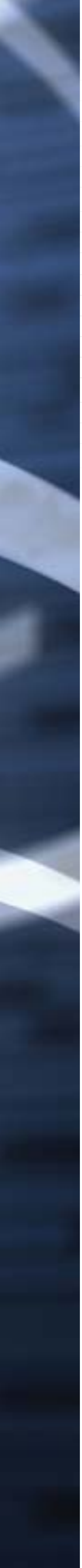
Larger companies – and some public bodies - need a dedicated DATA PROTECTION OFFICER

The regulations recommend use of TECHNOLOGY TO LIMIT RISK

The GDPR has already been adopted as UK law and we must all be **GDPR compliant by May 2018.** It's a complicated piece of legislation... and the clock is ticking...but there is much that can be done.

- Brings in a '**right to erasure**' - people can ask for all their data to be removed from systems
- People have **right to bring individual law suits** and make compensation claims
- Legislation **affects everyone that handles EU citizens' personal data** – no matter if they're inside or outside the EU

avatu



Five steps to GDPR compliance

72 hours of its discovery

Identify #1

To develop an effective defence strategy, the first step is to understand your data. You need to be clear whether your organisation is a data controller or a data processor when it comes to personal data. Personal data is any information that can potentially identify someone, and the GDPR widens the definition compared to the current Data Protection Act.

Organisations must regularly review existing and new processes around personal data. They need to understand where this data resides, and who has access to it. It's also important to understand how it's used: when it's at-rest, in-motion and/or in-use. Knowing this will help them to understand how this data is/should be protected.

There is technology which can help assess and manage unstructured data and massive data sets and reduce the burden of this task.

Protect #2

Having identified data as personal data, it is vital that it is secured. Common control standards include encryption and access control. But this alone is not sufficient. Monitoring potential data leaks, from negligent or malicious employees, and external data theft are also important considerations. Password sharing puts organisations at risk of data loss because people use passwords that are all too easy to crack.

To demonstrate compliance with the GDPR, alternative solutions will need to be adopted. Technology which eradicates breaches via email attachments can significantly reduce the risk. Products which routinely control who sees what information and what they can do with it is another layer of mitigation. Tools which continually educate employees and stop them making data vulnerable can also limit exposure.

Detect #3

When a data loss occurs, it's critical that the breach is detected quickly so you can know if any personal data records were lost or stolen. If they were, rapid notification is paramount. Notifications must be sent to the ICO within 72 hours of its discovery and a full investigation needs to be started.

Organisations need to design protection strategies for the differing levels of sensitivity of their data. They need tools that will not only protect the organisation's 'crown jewels', but also minimise the chance of a data leak.

It is widely acknowledged that it takes an average of 247 days for organisations to discover that they have indeed been breached, and the UK average is believed to be more like 400 days, according to recent government research. This is mainly because the industry focus has traditionally been on creating perimeter defences, such as anti-virus and firewall technologies. Unfortunately, these will only help to defend against known threats.

Next generation tools that use 'deep inspection' techniques to detect all breaches in real-time, enable quicker response and reduce the impact of a data breach.

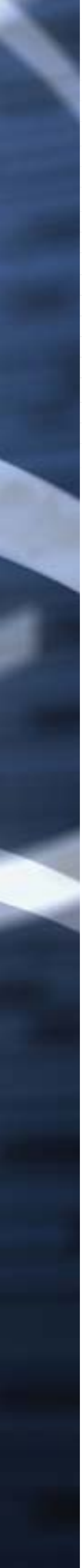
Respond #4

The GDPR means that security breaches can no longer be swept under the carpet. Incident response is a crucial element when it comes to protecting the data and mitigating damage. On top of the mandatory data breach notification requirement, organisations must also make sure they've implemented and tested an effective incident response plan. With a plan in place, organisations have a better chance of reducing the impact of data breaches.

A robust – tried and tested - incident response plan will help organisations prepare to tackle a crisis head on. Digital forensics will be an important part of finding out what has happened and who is responsible, and provide intelligence to improve future protection. It will also be an opportunity to iron out any issues for business continuity and minimise future risk.

Recover #5

The final step for businesses that fall victim to a data breach is to continue ongoing communication with a variety of audiences, including the ICO, the customers effected, investors and the wider customer base. This makes sure any losses are managed and those who have been directly effected are regularly kept informed. During the recovery process, organisations will learn the lessons of why things went wrong, and should rebuild as a stronger more data savvy organisation. This part could also effect the scale of any sanctions handed down by the ICO.



Innovative technology will be key to GDPR compliance

The Information Commissioner Elizabeth Denham has said that one of her office's strategic priorities is to 'explore innovative and technologically agile ways of protecting privacy'.

Specific articles within the GDPR also refer to using technology to assist in compliance.

Places where innovative technology can help with the GDPR include:

✓ Can help organisations understand the data they have and prioritise it

✓ Can prevent unauthorised processing of personal data (as mentioned in Article 5)

✓ In case of a breach, can support notification of the supervising authority within 72 hours (as mentioned in Article 33)

✓ Can show you've mitigated the risk in case of a data breach

✓ Can help regularly assesses your GDPR compliance (as mentioned in Article 32)

✓ Can demonstrate your GDPR compliance (as mentioned in Article 24 & Article 39)

✓ Can add layers of security that protect personal data from data loss

✓ Can increase awareness/training for staff involved in processing operations and related audits (as mentioned in Article 39)

> Many companies are looking at it as a prompt to look at their data security as a whole.

If a breach happens: A legal review of the risks

If you do suffer a data breach, there are factors which will make the situation better or worse for you.

They include:

- The nature, gravity and duration of the breach
- The number of data subjects effected and damage suffered
- The categories of personal data effected by the breach
- If the breach is intentional/negligent (ignorance is no defence)
- If remedial action has been taken
- If appropriate security measures were in place
- Was there a previous history of breaches
- The degree of co-operation with authorities
- How the ICO became aware (was it by self notification/whistle-blower/GCHQ?)
- Was there compliance or non-compliance with previous enforcement orders
- Was there adherence to codes of conduct/certification schemes
- Has there been Ill-gotten gain from the breach
- How swiftly was it notified or detected

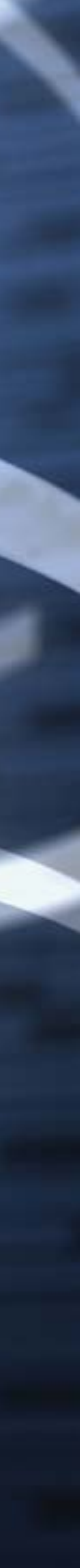
The positive thing is, however, you can deal with many of these now.

Still unclear about the **GDPR** and how it **effects you**? Need advice on technologies that can help?

Anyone who has questions about the GDPR, or who's unclear about their readiness for the new rules, can arrange a **special free gap analysis assessment** with Avatu or signup for an Avatu GDPR webinar or briefing.

We can also brief you on innovative technologies that can help with your commitments and reduce your risks.

Phone 01296 621121 email: cybersecurity@avatu.co.uk



The 8 things you should be doing right NOW

1. Make sure people at all levels of the business know about the GDPR, its requirements and the implications of getting it wrong

Make sure that decision makers and other key people in your organisation are aware that the law is changing. They need to appreciate the impact this is likely to have and give it the right emphasis and investment. Brief them on how technology can ease some of that burden.

2. Understand your data

Find out what you hold, where you hold it, who has access to it and how it's protected right now (if at all). Without knowing this, you can't make considered data security decisions. The GDPR is aimed at being risk based. You can't know which data is the most risk laden if you don't know what you've got. Consider how you would deal with a request for erasure. Think about the layers that are needed to protect your most sensitive or vulnerable data. This is a daunting prospect for many. But there are technical solutions that can help.

3. Prepare for data security breaches

Establish clear policies and well-practised procedures to ensure that you can react quickly to a data breach and notify in time where required. Consider how you minimise the impact of a breach, and therefore exposure to risk.

4. Assess how you can minimise the chance of a data breach

Restrict access to sensitive data through such things as privilege management and digital rights management. Reduce the risk of data leaks by adding layers that deal with the vulnerabilities in emails and their attachments. Research deep dive analysis tools, which would catch threats much quicker than with traditional perimeter tools such as anti-virus.

5. Review your policies and procedures

You should review your current privacy notices and put a plan in place to make any changes needed because of the GDPR. The GDPR says that information provided should be in clear and plain language. Your policies should be transparent, easily accessible and easy to follow.

6. Create a framework for accountability

Appoint a data protection officer, if needed.

Develop a data-conscious culture. This should cover monitoring, reviewing and assessing your data processing procedures. Check that your teams are trained. Consider technology that reinforces the training and constantly keeps it at the forefront of people's minds. It can ensure that people work within your policies and procedures and your data remains safe.

7. Get legal advice on how you're using data now, and consider how you want to use it in the future

Allen & Overy lawyers recommend that you consider what data processing you undertake. Do you rely on data subject consent for example, or can you show that you have a legitimate interest in processing that data that is not overridden by the interests of the data subject? Companies often assume that they need to obtain the consent of data subjects to process their data. However, consent is just one of a number of different ways of legitimising processing activity and may not be the best (eg it can be withdrawn). If you do rely on obtaining consent, review whether your documents and forms of consent are adequate and check that consents are freely given, specific and informed. You will bear the burden of proof.

8. Embrace privacy by design and become familiar with privacy impact assessments

Make sure that privacy and data security is built into everything new you do. You should familiarise yourself with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

> Companies should solve data security issues by approaching them from a pragmatic, business point of view. The introduction of the GDPR has provided organisations with an opportunity (if not a wake-up call) to take full control of their data and re-evaluate security systems that are no longer suitable.

avatu

www.avatu.co.uk
phone 01296 621121

Still unclear about the GDPR and how it effects you?
Need advice on technologies that can help?

Phone 01296 621121 email: cybersecurity@avatu.co.uk

Sources: The ICO strategic plan 2017-2021, published April 2017 | The General Data Protection Regulation, numbered Regulation 2016/679| The New Statesman Policy Report on Cyber Security February 2017 | GDPR legal update 360 Business Law, March 2017 | Preparing for the General Data Protection 12 Steps to take now, ICO |Allen & Overy, The EU General Data Protection Regulation 2017