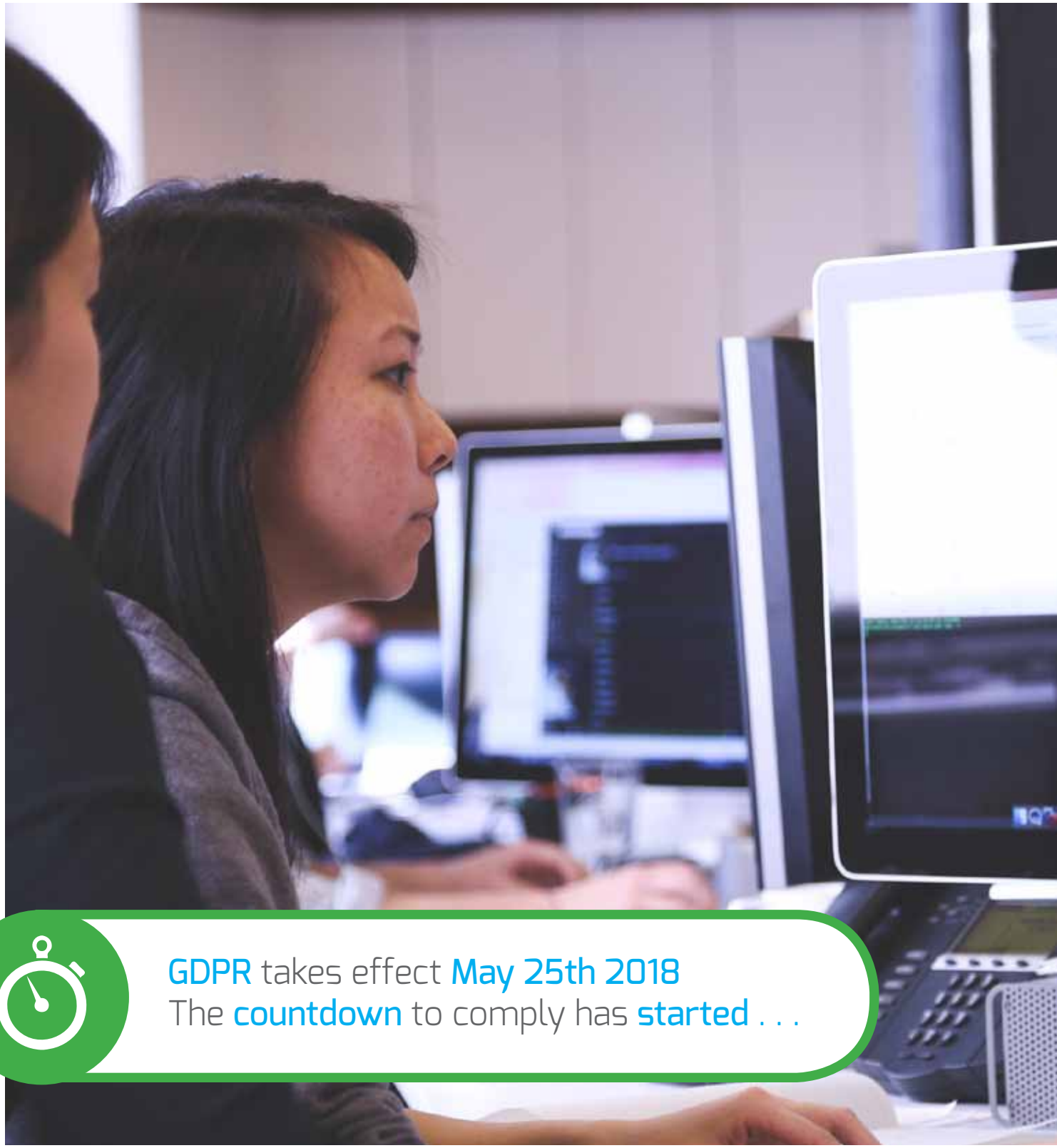
NCi TECHNOLOGIES

IT Solutions for
Business & Schools

How to Prepare your **Business** or **School** for **GDPR**

Are You Ready?



GDPR takes effect May 25th 2018
The countdown to comply has started . . .

Microsoft Partner

What is GDPR?

The General Data Protection Regulation (GDPR) (Regulation (E.U.) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (E.U.).

At the same time it will ensure companies themselves have a clear and dependable set of rules when handling data.

Ratified in April 2016 the regulation will replace the Data Protection Act 1998 and cover the capture, control and consent to use personal information.

In simple terms, GDPR is an enhanced version of the Data Protection Act 2018 covering any company inside or outside the E.U., that offers goods and services to European citizens. It's highly likely your organization must comply with GDPR.

Brexit and GDPR

In 2018 the UK will still be an E.U. member state and must comply with the regulation. When Brexit happens, in order to be a tradeable nation we will still need to comply as will any country outside of the E.U. who wants to trade within it.

The intention of the regulation is clear. It is in place to protect personal information and puts the responsibility of protecting the personal data of employees, customers and prospects firmly on the shoulders of your organization.

Fines of the greater of €20m or 4% of **worldwide annual** turnover can be imposed by regulators for **breaches** of the **GDPR.**

GDPR – What's new at a glance …

Much larger fines for none compliance/ none readiness / actual data loss – currently UK fines are a maximum of £500,000

The right to Erasure and be forgotten – the subject has a right to withdraw consent for companies to hold their data at any time.

Timely Breach notification – within 72 hours of data loss.

Expanded territorial scope - all data controllers and processors are subject to the GDPR if the operate within the E.U. or hold data on E.U. citizens.

Consent will be harder to get – subjects must now opt in to having data held on them rather than opting out as previously and must be provable as a clear affirmative action.

Plus more…

Personal Data

Cybercrime is no longer about inconveniencing computer users by making the letters in documents you type drop into nice looking pyramids, nowadays individuals, businesses, even whole countries can be held to ransom.

In our current technological climate, the global economy runs on data, data that continues to grow at alarming rates and the truth is …. The digital age needs a new set of data rules.

Consider the personal data that you freely give online when purchasing goods.

- Name
- Address
- Birthdate
- Credit Card details
- Usernames
- Passwords
- Email addresses
- And more

Now think of the value of that data to someone who may want to benefit from it.
Again consider the information captured in the background without you even noticing:

- Your IP Address determining where in the world you are logged on
- Your search history
- What you bought, now and previously
- Items you frequently look at or search for
- What web pages you view and how long you stay on each page

Think about the data you hold on your staff

- Curriculum Vitae's
- Start dates
- Holiday information
- Sickness
- Pay and bonuses
- HR related information
- Appraisals, warnings etc.

As the value of that data increases so does the determination of the very people who want to access and use that data for their own purposes.

Data Breaches

In 2016 over 2 billion records were reported stolen.

There were 974 publicly disclosed data breaches in the first half of 2016, which led to the successful theft or loss of 554 million data records.

3.04 million records compromised every day

126,936 records compromised every hour

2,116 records compromised every minute

35 records compromised every second

Identity theft accounted for 64% of data breaches in 2016 with 9% of attacks coming from inside the organisations.

Why should it concern me?

On the 25th May 2018 when the regulation comes into effect it's NOT a gradual phasing in.

YOU NEED TO BE COMPLIANT!
Or risk heavy fines.

You could be put out of business with a single violation either financially, or by damaged reputation.

Are you a charity, health organisation, business, school, marketing agency, website? It doesn't matter, to be fair, if you hold or manage data on any E.U. citizen getting compliant and ensuring continued compliance should be your priority.

What should I do about it?

OK you have scared me what should I do about it?

Our job isn't to scare you, or direct you down paths that are not good for your business. Our job is to support you, to keep you secure as much as we possibly can with the resources we have at hand, but we can't do that alone. YOU have to take responsibility for your data both externally and internally.

Just some of the things you need to consider:

Do you hold or store personal or sensitive data in your organisation and if so where do you store it?

Typically an organisations data is classified as follows:

20% Mission Critical	30% Redundant	50% Indeterminate Value

Who has access to that data and how secure is that access?

1. Do you use multi factor authentication?
2. Are all your operating systems and applications regularly updated and patched?
3. Are your server group policies implemented and managed
4. Do you allow external organisations access and what are their security policies?

Is your network as secure as it could be?

1. Do you have a firewall and if so what features on it are managed and updated?
2. Do you use a recognised reliable anti-virus across your whole organisation?
3. Do you monitor data traffic on your network?
4. Have you implemented Bring Your Own Device (BYOD)?
5. Is there a data loss prevention strategy? – anti-virus keeps the bad stuff out, data loss prevention keeps the good stuff in.

What should I do about it? Continued

How do you manage your email?

1. Do you use and manage archived email?
2. How secure is your email?
3. Where is your email stored?
4. Who has what access rights to the companies emails?
5. Do you monitor the companies email?
6. What are your company policies on email usage?

91% of cyber attacks begin with a phishing email

How secure is your data on and offsite?

1. How is personal/sensitive data taken offsite transported/stored?
2. Is it encrypted?
3. Do you allow unencrypted laptops/USB sticks on to your network?
4. Is your server encrypted?
5. What authentication is used to log on to your network?
6. Do you use CCTV? Who has access to the files and is that secured?
7. How long do you keep archived data?
8. Do you Pseudonymise identities?

Do you backup your data?

1. How often?
2. On to tape or disk?
3. Is it secure or encrypted?
4. How easy is it for 3rd parties to recover if found?
5. Is it kept onsite or offsite or both?
6. If offsite do you know where?
7. Who has access to the data offsite?

More Information

This information is not exhaustive. It is designed to get you thinking, to get you on the road to compliance and to help us help you make your business secure. We are not experts in GDPR but we are experts in I.T.

If you need help or advice preparing your business or school to be secure now and for future years whether it be encryption, web filtering, multi factor authentication, data backup, email security or any of the other endless security concerns then please contact us.

GDPR doesn't take your budget as an excuse for non-compliance – but can you afford not to be compliant.

NCI TECHNOLOGIES

Cloud Services | IT Support Contract | Security | On-site Installation | BDR | Broadband | Telephone Systems | IT Procurement

NCI was founded in February 2004, by Directors Andy Trish, Chris Penrose and John Andrew, with a vision to provide great IT support to the local community. Over the last decade, the company has grown considerably and is now a 30 strong team of passionate and dedicated professionals delivering IT solutions to businesses and schools across the UK.

NCI continually strive to improve their services and increase customer satisfaction. Years of experience working closely with small and medium sized businesses and schools have led NCI to develop products and services that empower their customers to progress and lead the way.

Microsoft Partner
Gold Volume Licensing

Microsoft Authorised Education Reseller
Gold Partner

01326 379 497
info@ncitech.co.uk
ncitech.co.uk
esafetymatters.co.uk