THE CONTRACT DOCTOR

COMPLIANCE CURED

GDPR TIPS

Here are some tips with regards to your computer & physical environment at the office and at home. The below will help you spot and prevent potential data breaches.

THE CONTRACT DOCTOR
COMPLIANCE CURED

Be Proactive

Simple security measures are effective and only take a small investment in time to implement. Consider the following:

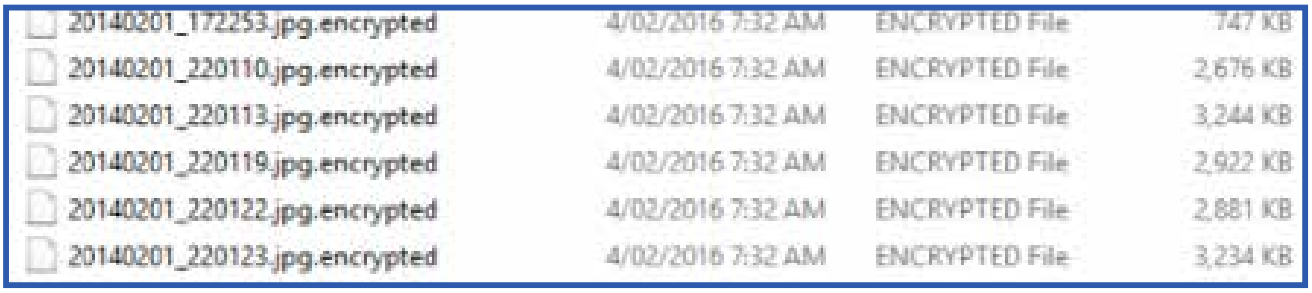
- Have you saved documents to your local hard drive that should be in a secure shared (server) location where only those with authorised access can view it?
- Have you downloaded a copy of a C.V and left it in your downloads folder?
- Can your computer monitor be overlooked by anyone that should not have access to the personal information displayed on it?
- Do you have a very strong password that you do not share with others?
- Does your computer have its firewall switched on and is the anti-virus up to date?
- Do you regularly install the updates that are provided by the software developers as these are often security patches?

Maintaining your company's compliance will rely on an element of you being proactive in keeping the personal data you process, secure and out of harm's way.

Be Alert

Cyber criminals look to access computer systems through false and deceiving emails, typically these are called Phishing attacks. Unfortunately, it is often the human link in the chain that is easiest to deceive often with costly results.

Being alert to emails with unfamiliar attachments, unusual instructions, misspelt text etc. will reduce the opportunity for cyber-attacks to succeed. However, you need to be on guard for potential breaches and spotting a crypto file (such as the one in the image below) will maximise your chance of capturing the infection before it has encrypted all your files. Regular backups of your computer drive(s) will allow you to reinstate your systems and data without paying a ransom to the cyber criminals.



The security of data doesn't just apply to the ability to access computer files, but also all other means of storing personal information. Despite the clamour for the 'paperless' office of a generation ago, the reality is that most organisations store paper files containing personal data. Here are some easy to implement measures that will help you keep your data secure, whether it's in a filing cabinet, on your server or PC/ Laptop hard drive.

- Ensure there is adequate control over the access to your work area to prevent unauthorised persons accessing data. This could be mechanical or electronic door locks, reception desks etc.
- Make sure visitors are escorted and display visitor passes
- Files containing personal information should be locked in cabinets when the offices are unattended
- Server rooms or cabinets should be locked with access limited
- Maintain a clear desk policy to avoid unauthorised access to personal data
- Consider the layout of the office, particularly if the public have access to ensure personal information cannot be casually overseen.
- Do not leave keys in cabinets or desk pedestal locks

These simple measures will help reduce the risk of data breach

Homeworking:

THE CONTRACT DOC+OR
COMPLIANCE CURED

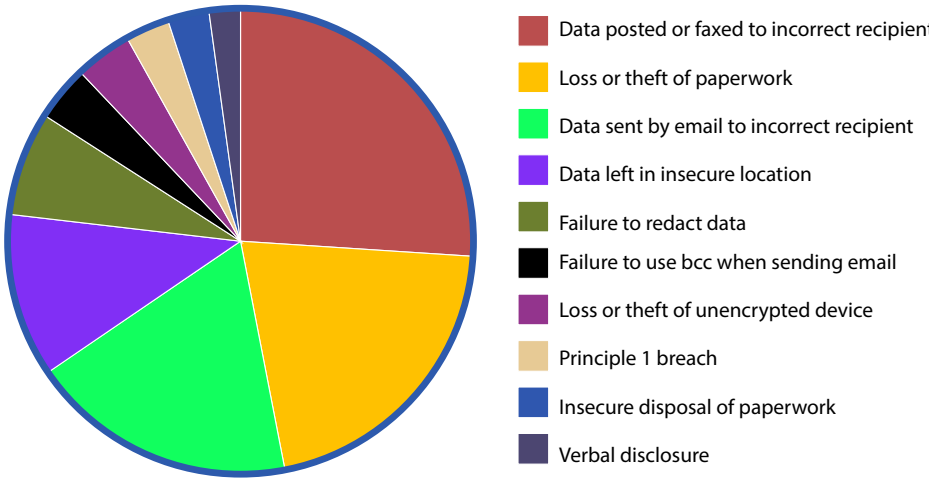
Firstly, secure your technology!

- Create strong passwords
- Never disclose your passwords
- Use 2 factor authentication onto those systems that provide it
- Make sure your anti-virus and anti-malware protection is up to data and operating
- If your operating system (such as Windows 10) as an encryption feature, switch it on
- Ensure your internet router has a secure password
- If you have to save personal data to your laptop, device or computer, delete it once you can upload it to the company network
- Wherever you can, use a separate device for work and home

Secure your home office!

- Keep paper records out of anyone else's sight
- Lock away paper records when not working
- Ensure your computer screen locks and requires a password if you leave your desk
- Lock doors and put devices out of view if you leave your house
- Don't let anyone 'shoulder surf' behind you whilst working.
- Don't be fooled!

Be aware of suspicious looking emails, which ask you to click links or claim to be from a senior member of the company asking you to approve the transfer of large amounts of money. If you are unsure of the origin of an email, do not open it but report it to your IT support provider.



When it comes to GDPR , most people think its only the big things that count as a breach – how many of the above are we guilty of committing by mistake or just don't know the rules around GDPR.

OneMoreLead

August 4, 2021: A marketing company, OneMoreLead, has exposed the personal records of 126 million individuals through an unsecured database posted online. The database contained names, job titles, email addresses, work email addresses, home device IP address, home address, work address, personal phone number, work phone number and employer.

Sony Interactive Entertainment

Formally known as Sony Computer Entertainment Europe, this company is a multinational video game and entertainment provider. The hack took place in 2011, where personal information of close to 80 million customers of Sony's PlayStation Network, including names, addresses, date of birth and account passwords. Along with payment card, details were exposed.

The Consequences:

The Information Commissioner's Office (ICO) hit the company with a 250,000 pound fine for breaching the Data Protection Act by not having up to date security software. The ICO stated that it could have been preventable, were Sony to have been operating in lines with the Data Protection Act. With an official apology shared by the company's officials, users were also offered free games, in an attempt to keep the customers on board.

Tesco

Tesco bank is a British retail bank that was formed in a joint venture between Tesco, the largest supermarket in the U.K, and The Royal Bank of Scotland. In 2016, close to 10,000 customer accounts were hacked where money was taken from them, in a total of 2.5 million pounds. The money that was extracted from customers' accounts was fully reimbursed by the company. With not much information shared about how the attack took place, it was shared that it involved gaining access to debit card information of customers, in the online banking area of the company. Some theories suggest it was an internal security breach, though it is largely unknown what exactly took place without Tesco sharing the details of the hack. The attack was made up of transactions from an outside source, most of which were from Brazil. The fraud security team at Tesco attempted to ban these transactions, but an error was made, and the transactions continued to take place until eventually, the team was able to stop the hack, two days after it was noticed.

The Consequences

Losses amounted to 2.5 million pounds that had to be repaid by Tesco to the customers affected. As soon as the news hit, shares in the business dropped by 3% and continued to drop weeks after the attack. Tesco was eventually fined 16.4 million pounds by The Financial Conduct Authority, 2 years after the attack took place.

THE CONTRACT DOCTOR

COMPLIANCE CURED

Let's talk!

Get in touch with The Contract Doctor today!