Archive Document Data Storage

GDPR Compliance: A Brief Data Protection Checklist

One of the biggest parts of the GDPR legislation is the protection of your data and your response time to a data breach. The ADDS record centre sites have already had data breach prevention procedures in place for many years. Many of our clients ask us for tips on how to prevent a data breach and we remind our clients that data breaches do not only occur via a lost laptop or network hack, they can also occur internally within the organisation.

Below is a small sample of a checklist that you may wish to use and add to. We have compiled a sample list of questions every manager should be asking themselves to reduce the risk of a data breach. If the answer to any of these questions is no, how can you make changes to adapt and fix potential issues before they occur?

Please remember that this is just a sample of one of the tools we use at ADDS. It is not legal or consultation advice, just a little helping hand to move you in the right direction…

Site Access & Security	Yes	No
Do all team members sign in and out of site?		
Do all team members wear company-issued photo ID?		
Are team members across all departments and levels security checked?		
Do all team members receive 'welcoming training' as part of your building security process?		
Are security checks repeated at regular intervals?		
Do all suppliers and clients sign in and out of site?		
Are suppliers and clients issued with a security process on check-in?		
Do you ask clients and suppliers to provide photo ID upon entry to the building to verify that they are who they say they are?		
Are clients escorted on-site at all times?		
Are suppliers escorted on-site at all times?		
If there was a data breach, would you be able to pull a list of all people on-site at that time and date?		
Think about how you contact external parties who have been on-site. Do you have their permission to hold their data?		
Are open windows within the office area left unattended throughout the day?		
Are exits / fire exits checked regularly throughout the day?		
Do you have CCTV that covers access points to and from your office? Consider how long the CCTV is retained for.		
Have you ever tested the CCTV system to recall footage?		

Office Closure Process

	Yes	No
Is there a process for the last person who leaves the building / department that can be ticked off and documented as complete? E.g. Windows closed? Desks clear? Computers switched off? Storage cabinets locked?		
Do you have a process to secure your office at night? Consider who has access.		
Do you have access to a record of who has locked up every evening?		
If you have a cleaning company servicing your office out of hours, do the cleaning company run security checks on their team members?		
Do you have clear desk policy or do the cleaners have access to confidential information when you are not there?		
Do the cleaners regularly change? Ideally, the same cleaners would be on-site each day.		
Do you request your cleaning company to notify you of who will be attending?		
Do you ask the cleaning staff to provide photographic ID and sign in and out every day?		

IT Security

	Yes	No
When you assign IT equipment to team members, is it documented?		
Do you have an IT asset management inventory?		
Do you run IT equipment audits regularly?		
Do you regularly audit your team's PC and laptops for locally stored documents? Best practice is that documents are not locally stored.		
Do you regularly audit laptops and PCs to make sure Windows updates are up-to-date and antivirus software is scanning every day?		
Are your team consistently reminded to run daily security scans on their PC and laptops?		
Do team members sign a document to say they have run a security scan daily?		
Do you request that team members create strong passwords, such as a combination of upper and lower case, symbols and numbers?		
Does your system request a password change every 30 days at least?		
Are your team members regularly trained on IT security and password security?		
Are team members in the practice of regularly locking their PCs and laptops when they leave their desk?		
Do your team members regularly empty their laptop/PC recycling bins?		
Do you have a clear process in place to report a company laptop as lost or stolen?		
Have you deactivated access to social media sites? We all like some internet freedom but the hazards that social media sites and personal email logins like gmail can provide to an IT network can be devastating.		
Do you control portable media devices on PC and laptops to avoid team members plugging in their USB sticks and running mass data downloads without IT consent?		
If your team members are issued work mobile phones, have they been trained to secure the phone with auto screen locks?		
Do you collect IMEI numbers for IT asset management?		
If your server is situated at your site, does it have extra security and controlled access?		
Is the server room kept locked at all time?		
Is access to the server room monitored?		

Disposal of Paperwork

	Yes	No
Is there a process in place for secure destruction?		
Is paperwork securely shredded with a professional shredder?		
If you have serviced secure destruction cabinets on-site, do all team members know where they are located? Best practice is to clearly label them so that they are not confused with recycling bins.		
Are the secure destruction cabinets regularly serviced?		
Does your secure destruction supplier have ISO 127001?		

On-site File Rooms

	Yes	No
If you have an on-site file room, is there a strict access process in place?		
Are all files barcoded? Can the file barcode provide a complete audit history?		
Is the on-site file room audited at regular intervals?		
Do you use an auditable barcode-tracking system to monitor if files have been returned to the file room?		
Does the on-site file room have additional security, such as its own alarm zone?		

The list of questions above are not exhaustive, but they serve as a guideline to organisations trying to reduce the risk of a business-crippling data breach occurring.

For further useful information about the GDPR, please visit our GDPR page:

www.archivestorage.net/news/gdpr