Solve IT GDPR Checklist

Policies & Procedures

❑ Register with Data Protection Commissioner.

❑ Appoint Data Protection Officer “DPO”

❑ Conduct staff training on confidentiality and privacy.

❑ Ensure confidentiality clause is present in staff contracts or separate Non-Disclosure Agreement, “NDA”, is in place.

❑ Put in place a NDA with your hardware and software support companies and any other entity accessing information.

❑ Add disclaimer to all outgoing emails.

Access Control

❑ Require password access on all PCs and Servers

❑ Ensure all users log in with their own user name and password

❑ Ensure all users log out – lock PC when they are away from their desk.

❑ All accounts should have ‘strong’ passwords and must be changed every 90 Days

❑ Permissions set to only allow authorised staff to access data.

❑ Ensure your software systems provides an audit trail.

❑ Ensure the physical security of both paper and electronic records.

Managing Devices

❑ Encrypt the hard drive of any laptops or mobile devices that hold client records.

❑ Encrypt the hard drives of all Servers.

❑ Auto shutdown all PCs at night.

❑ All PCs to run latest version of Operating System.

❑ All PCs to have all security patches in place.

❑ Contract RMM Supplier for Monitoring and management.

❑ Anti-Virus & Malware software installed and updated on all PCs.

❑ Keep Firewall up to date. Use IDP and routinely examine logs.

❑ Don’t put client data on USB memory sticks unless the Stick is encrypted.

❑ Secure your Hardware environment. Lock the Comms Cabinets and Rooms

❑ Activate Mobile Device management on Office365 Tenants.

❑ Switch WiFi to RADIUS server. WPA Enterprise.

Information Security

❑ Do not remove any paper copies of data from the premises.

❑ Put in place a company policy on use of the internet

❑ Don't use email for sending client identifiable information unless its encrypted.

❑ Activate 2 Factor Authentication on all email accounts.

❑ Setup email encryption for accounts as needed.

❑ Enable Audit Log search on 365 Tenant.

Backups

❑ Backup all Data at least daily

❑ Store backups off site in a secure location. Use NAS in Separate Building

❑ Do a test restore on a regular basis

❑ Make sure all Online backups are encrypted.

❑ Clients to review Backups every 3 months, to ensure the correct data is being backed up.

Obtaining Information

❑ Give information leaflet on data protection to all clients.

❑ Use agreed data collection form for new clients.

❑ Make clients aware of their rights.

the right to be informed, the right of access, the right to rectification, the right to be forgotten, the right to restrict processing, the right to data portability, the right to compensation & liability.

❑ Do not collect PPSN unless required for a specific service.

Information Sharing

❑ Be careful and aware when asked to share client data.

❑ Ensure written consent is provided for every request.

❑ Ensure anonymity of records when carrying out audit or research

Data Retention

❑ Be aware of the data retention periods for different kinds of data.

❑ Implement a defined policy on retention periods for all data.

Data Breach

❑ Set out the incident report team responsible for dealing with a breach.

❑ Mandatory breach reporting done within 72 hours of the incident.

❑ Notify data subjects where the breach is likely to result in a ‘high risk’ to them.