GENERAL DATA PROTECTION REGULATION (GDPR) CHECKLIST

PHASE 1 - AUDIT YOUR SITUATION

- ☐ Find out about the data that you collect and make a note of it. E.g names, addresses, IP addresses, cookies.
- ☐ Make sure you obtained this data fairly with the necessary consents. Make sure you have asked for permission to be in possession of this data.
- ☐ Make sure your data is safe and secure with appropriate levels of security.
- ☐ Find out if your service partners, that have access to your data, are GDPR compliant.
- ☐ Audit all authorized and unauthorized devices that have access to personal data.
- ☐ Audit all your devices to see what is old and new. Remember, some manufacturers will not release security updates for old software and hardware, causing a potential security risk.

PHASE 2 - ACCESS CONTROL

- ☐ List who has administrative privileged control to your data.
- ☐ Find out if your user accounts are set on levels of privilege for certain data sets.
- ☐ Make sure you can retrieve and erase data from devices with access to personal data.

PHASE 3 - ROBUST SECURITY

- ☐ Invest in an efficient and reliable anti-virus for your network and devices.
- ☐ Invest in a trustworthy and effective anti-malware software for your network and devices.
- ☐ Invest in a dependable firewall for your network and devices.
- ☐ Backup your data. Make sure you have considered more secure and robust methods of backups, such as in-house and online/cloud backups.
- ☐ If you have a form of backups already, look at how secure those backups are.

Comms-Byte Ltd, Davenport House, 251 Wellington Road, South, Stockport, SK2 6NG
Telephone: 0161 820 8980 Email: sales@comms-byte.com
Comms-Byte Ltd registered in England and Wales no: 03063530, VAT No: 638 9675 74

GENERAL DATA PROTECTION REGULATION (GDPR) CHECKLIST

☐	Consider a Disaster Recover as a Service solution.
☐	Invest in a Patch Management Strategy. Regular updates and scans are very important to keeping out potential risks to your data and systems.
☐	Upgrade all old devices and software to take advantage of the new security updates and features.
☐	Take all necessary physical security precautions. Physically, consider how safe your business data is.
☐	Educate your staff on the importance of cybersecurity. Speak to your staff regularly to test their knowledge on recognising attacks and taking precautions to avoid security risks.
	PHASE 4 - DOCUMENTATION
☐	Have a Privacy Policy in place and update this to reflect your current situation and to make it legally compliant.
☐	Have an updated Password Policy and make sure you and your staff follow this.
☐	Document any previous data breaches.
☐	Document all internal procedures.
	PHASE 5 - ADDITIONAL REQUIREMENTS
☐	Report any data breaches within 72 hours.
☐	Prove due diligence in preventing future breaches.
☐	Provide personal data to all EU citizens who ask for it in an appropriate format.
☐	Upon the citizen's request, erase all their data.
☐	Make sure you only transfer data to GDPR compliant organisations or to those deemed 'adequate'.

Comms-Byte Ltd, Davenport House, 251 Wellington Road, South, Stockport, SK2 6NG
Telephone: 0161 820 8980 Email: sales@comms-byte.com
Comms-Byte Ltd registered in England and Wales no: 03063530, VAT No: 638 9675 74