Fellowes

Business Checklist

Supporting **GDPR** compliance and alignment with **NIS2** regulations

Supporting Staff Compliance

1 Keep policies up to date

- Review BYOD rules and include guidance for home working.
- Address risks of public/home Wi-Fi and how staff should connect safely.
- Update policies on printing, storing, and disposing of paper documents (office & home).
- Strengthen password guidance (e.g., three-word passphrases, MFA).
- Require secure erasure of all data before disposing of IT equipment.

2 Provide regular training

- Educate employees on GDPR basics, data handling, and the six principles of data protection.
- Include handling of sensitive paper documents and retention rules.
- Add modules on home office security and new policy updates.
- Use an online training portal to track completion and deadlines.
- Provide practical tools such as a checklist or self-assessment "Data Security Health Check."
- Refer to NIS2 in training as an added layer of cyber resilience, especially for IT and security teams.

3 Equip employees properly

- Provide company laptops instead of relying on personal devices (BYOD).
- Invest in strong antivirus and firewall systems.
- Ensure access to shredders: office-grade in the workplace and compact shredders for home use.
- Use micro-cut (P-5) shredders for highly confidential data.
- Prioritise productivity and safety features (e.g., jam prevention, safe operation).

4 Communicate consistently

- Reinforce security at all levels; close knowledge gaps for junior staff.
- Cover data security in site meetings, team huddles, and 1:1 check-ins.
- Share policy updates via posters, newsletters, and intranet.
- Circulate phishing/cyber-attack alerts and best practices across the business.
- Make data security a standing item in quarterly business reviews.
- Position GDPR as the compliance foundation, with NIS2 referenced where it strengthens cybersecurity culture.