green pepper

Checklist

Reviewing Your GDPR Compliance

Privacy Rules

- [ ] Are you aware of the data protection principles?
- [ ] Are you aware of the lawful bases for processing personal data?
- [ ] Are you aware of the privacy rights of individuals?
- [ ] Are you aware of the special rules regarding consent and automated direct marketing?
- [ ] Are you aware of the rules for processing special category or criminal conviction data?

Compliance

- [ ] Have you assessed the data processing operations that you perform?
- [ ] Have you assessed the privacy risks of your data processing?
- [ ] Have you decided upon the legal bases that allow you to perform each data processing operation?
- [ ] Are your data processing operations transparent, and explained in a privacy statement?

Consent

If relying upon consent as a legal basis for data processing…

- [ ] Has this been given by free, affirmative action?
- [ ] Has separate consent been sought for different processing operations?
- [ ] Are individuals told they can opt-out at any time; and is the easy for them to do?
- [ ] Can you produce evidence that an individual has given free and affirmative consent?

Privacy Statements

- ☐ Does your privacy statement include all the information required by law?
- ☐ Is your privacy statement made freely available to individuals at the point when data is collected, or very soon afterwards?
- ☐ Is your privacy statement concise, intelligible, and free of jargon?

Security

- ☐ Is access to personal data sufficiently controlled?
- ☐ Do you have sufficient physical security to protect areas where personal data is stored?
- ☐ Do you have a process for the safe disposal of unwanted personal data?
- ☐ Do you have guidelines on the use of passwords?
- ☐ Do you keep regular back-ups of all your personal data?
- ☐ Do you have sufficient cyber security to protect against malware, phishing and other forms of cyber attack?
- ☐ Do you have procedures for ensuring the security of laptops and other mobile devices?

Policies and Procedures

- ☐ Are key responsibilities documented or made clear to all involved?
- ☐ Do you have a written policy for the processing of special category or criminal conviction data?
- ☐ Do you have written contracts with any third party data processors, and do they meet the requirements of data protection law?
- ☐ Do you have a procedure that sets down when and how personal data can be processed when the safeguarding of vulnerable adults or children is relevant?
- ☐ Do you have a procedure to record and report data breaches?
- ☐ Do you have a procedure to handle complaints regarding the privacy rights of individuals?

Staff and Volunteers

- ☐ Are all staff and/or volunteers fully aware of the importance of protecting privacy?
- ☐ Have all staff and/or volunteers who process personal data been properly trained on your data security and any other related procedures?

Governance

- ☐ Is there someone in your organisation with overall responsibility for data protection (or have you designated a data protection officer, if applicable)?
- ☐ Do you have proportionate governance measures in place to review and update your data protection policies and procedures?
- ☐ Do you document your data processing activity and keep appropriate records?
- ☐ Do you have the means to detect a data security breach?
- ☐ Are you satisfied you can demonstrate compliance with data protection law?

T. 01858 456211 https://greenpepperconsulting.co.uk