green pepper

Checklist

Are you GDPR compliant?

Introduction

The following checklist is designed to help you assess your current state of compliance with the GDPR and 2018 Data protection Act; and to consider where you need to take steps. It should be used in conjunction with guidance on data protection from a reliable source such as the ICO.

Data audits

- ❏ Have you undertaken a personal data audit?

  (Think about all the different activities that might lead to data capture such as fundraising, recruiting and managing volunteers/staff, dealing with beneficiaries, running events, policy forums, membership activity, direct marketing, campaigning, etc.)

  1. what is collected and how?
  2. when and where is it processed?
  3. what is it used for?
  4. who is it shared with?
  5. how is it stored, and for how long?
  6. is it needed?
  7. could it be anonymised?
  8. What are the privacy impacts of the processing?

- ❏ Have you recorded the outcome of your data audit in writing?

The lawful basis for processing

- ❏ Have you decided upon and documented the lawful basis that applies for each way that you process personal data?

- ❏ Where you process special category data, have you also identified a condition for your processing (see *Data Protection Act 2018* schedule 1)?

- ❑ If relying on consent (necessary for email marketing), has it been given freely, specifically, informed and unambiguously (no bundled purposes, pre-ticked boxes or opt-outs)?

- ❑ Where online consent is sought from children, do you have age verification/parental consent measures in place?

- ❑ Can you show that consent has been given by an individual?

- ❑ If relying upon a legitimate interest, have you undertaken a legitimate interest assessment?

  (When considering likely impact, you may need to think about the nature of the data and whether or not the subject is vulnerable in any way. If using this basis for telephone or postal direct marketing, you must also be able to offer an opt-out).

    1. We have identified the legitimate interest (purpose).
    2. The processing is necessary for that purpose.
    3. It does not override the interests of the individual.
    4. We have considered the likely impact; and our processing is not intrusive or harmful.
    5. An individual would reasonably expect such processing.
    6. By using the data, we would not be acting unethically or unlawfully.
    7. We would happily explain what we are doing to the data subjects.

Individual rights

- ❑ Are you aware of the full range of individual rights, and can you respond appropriately if needed?

- ❑ Do you make it clear to individuals that they can opt-out of direct marketing and is the process swift and simple?

- ❑ If you conduct automated decision making/profiling, are you aware of your extra responsibilities towards individuals, and can these be met?

Policies and procedures

- ❑ Have you updated your online and paper forms where consent is collected (to meet the strict requirements of GDPR)?

- ❑ Is your privacy notice transparent, clear and up-to-date?

- ❑ Does your privacy notice meet all the requirements of the GDPR with regards to content?

- ❑ Is your privacy notice made available to individuals at the point data is collected, or very soon afterwards?
- ❑ Do you have the means to detect, investigate and report personal data breaches?
- ❑ Do you have policies relating to data retention and to processing special category or criminal conviction data?
- ❑ Can you easily update or amend data in response to individual requests?
- ❑ If relevant, are your website cookie policy and processes GDPR compliant?
- ❑ Are you satisfied that other policies such as HR, marketing and procurement meet the requirements of the GDPR?

Security measures

- ❑ Is your data protected against unauthorised or unlawful processing (by physical and cyber security measures)?
- ❑ Do you have robust policies and procedures for the use of information technology within your organisation?
- ❑ Do you encrypt personal data that might cause distress or damage if lost or stolen?
- ❑ Is data security a priority feature of your policy on using laptops and other mobile devices?

Governance and accountability

- ❑ Is privacy embedded into your organisation's activities and procedures?
- ❑ Do you have proportionate governance measures in place in order to review and update policies?
- ❑ Do you document data processing activity and keep appropriate records?
- ❑ Is there someone senior with overall responsibility for data protection (have you designated a Data Protection Officer where required or desirable)?
- ❑ Where you use third party processors, do you have contracts that cover all the compulsory details set out in GDPR?

- ❑ If you undertake automated or processing that poses a high risk to individual rights, have you conducted a Data Protection Impact Assessment (DPIA)?

- ❑ If you transfer data outside of the EU, are you satisfied this is undertaken in compliance with the conditions set out in the GDPR; and do you document the details including the transfer mechanism?

- ❑ Overall, are you satisfied that you can demonstrate compliance with the GDPR?

Personnel

- ❑ Are staff and volunteers aware of privacy risks and the impact of a data breach?

- ❑ Do staff and volunteers understand the organisation's approach to data protection?

- ❑ Do staff and volunteers follow the organisation's policies and procedures concerning personal data?

- ❑ Have staff and volunteers been made aware of and trained in data security protocols?

- ❑ Do staff and volunteers know what to do if something goes wrong?