

GDPR ACTION PLAN TEMPLATE

Area	Task	Requirement	Template	Assigned Owner	Start Date	Deadline Date	Date Completed
1. AWARENESS & ACCOUNTABILITY	1.1	Instruct your workforce to direct GDPR related issues directly to you.					
	1.2	Train your workforce to record data in the right places.					
	1.3	Train your workforce on how to communicate with members.					
	1.4	Add GDPR training to your induction process and ongoing training programme.					
	1.5	Assess how your systems and processes look now, and how it needs to look to comply.					
	1.6	Ensure ongoing review of policies and procedures.					
2. INFORMATION YOU HOLD	2.1	Document the types of info you hold in your Information Asset Register.	Area 2 Template				
	2.2	Document where info comes from and the data flows related to its use within your Information Asset Register.					
	2.3	Document processing activities relating to special categories of personal data					
	2.4	Document your Data Retention Policy and ensure retention periods are captured in all privacy policies					
	2.5	Document who your data is shared with and identify if it is shared outside the EEA.9					
3. COMMUNICATING PRIVACY INFO	3.1	Update your Privacy Policy (you may require different versions for employees, volunteers, members (children) and contractors. This should include details of how individuals activate their rights.)	Area 3 Template A				
	3.2	Ensure your Privacy policy is published.					
	3.3	Update your internal Data Protection Policy and share with workforce so they are aware of what they can and cannot do with personal data. This should include information relating to IT, Security and use of remote devices.	Area 3 Template C				
4. INDIVIDUALS RIGHTS	4.1	Ensure individual's rights are listed in your Privacy Policy	Area 3 Template A				
5. ACCESS REQUESTS	5.1	Document how you'll handle people's requests for copies of their info.	Area 5 Template A				
	5.2	Document how you'll let people amend the info you have on them including consent.					
	5.3	Demonstrate how you will delete or 'forget' people from your records.					
	5.4	Document the file format and time scales these tasks will take.					
	5.5	Create Data request log	Area 5 Template B				

Area	Task	Requirement	Template	Assigned Owner	Start Date	Deadline Date	Date Completed
6. PROCESSING DATA	6.1	Document why you need to lawfully process people's data (Organisations with more than 250 employees will need to maintain a Register of Lawful Basis and Data Processing Activities)	Area 3 Template A				
	6.2	Document how you will ask people for permission to use their details.					
	6.3	Identify how you are going to treat any historic data you hold					
	6.4	Conduct and document physical security reviews of both IT and physical systems/records and their compatibility with GDPR					
	6.5	Ensure your asset register is accurate and up to date (if applicable)	Area 6 Template				
	6.6	Ensure you have additional security measures in place if processing special categories of data.					
	6.7	Ensure you have the necessary protections in place if data is being processed outside the EEA e.g. privacy shield etc.					
	6.8	Document your procedure for ensuring personal data is accurate and up to date					
	6.9	Ensure robust and frequent backups are in place for any IT systems and are retained for a sufficient period of time.					
	6.10	Ensure any 3 rd party processors have appropriate data security measures in place and you have data processing agreements in place with them.					
	6.11	If you act as a 3 rd party processor for another organisation (e.g. a club for a league) ensure you put a data sharing agreement in place.					
	6.12	Ensure you have the appropriate processes in place for destroying data when it is no longer required e.g. IT asset destruction, confidential waste destruction.					
7. CONSENT	7.1	Update Forms and data collection processes to ensure explicit consent is obtained where required	Area 3 Template B				
	7.2	Document how you will let people withdraw consent and document how easy this will be.	Area 3 Templates A&B				
8. CHILDREN	8.1	Document how you gain consent from parents / guardians of children.	Area 3 Templates A&B				
	8.2	Check your organisation management system / processes comply with NSPCC CPSU best practice guidelines for text / email broadcasts.					
9. DATA BREACHES	9.1	Document how you will deal with any potential data breaches.	Area 9 Template				

Area	Task	Requirement	Template	Assigned Owner	Start Date	Deadline Date	Date Completed
10. DATA PROTECTION BY DESIGN	10.1	Complete a Data Protection Impact Assessment (DPIA) as required.	Area 10 Template				
	10.2	If a DPIA is not required document the reasons for this decision. (Use Form 1 from the DPIA Tool)	Area 10 Template				
11. DATA PROTECTION OFFICERS	11.1	Decide if you need to appoint a DPO and record outcome and basis for decision.					
	11.2	If a DPO is not required set up a GDPR working group					
	11.3	Update job or role descriptions for those which have any addition Data Protection responsibilities					
12. INTERNATIONAL TRANSFERS OF DATA	12.1	If applicable, determine your lead data protection supervisory authority and document it.					