wood for trees

Rethinking Supporter Data
to Empower Change

Your GDPR Checklist

Charities will need to be fully compliant for GDPR by the 25th May 2018. This regulation is so much more than simply updating policies, procedures and processes. It is an organisation-wide responsibility with accountability and the individual's privacy at the centre of sweeping changes in data regulations. If you haven't yet started, now is the time to put your GDPR readiness plan into action. To help, we have created this checklist to guide you. To enable you to tick off those actions you've completed. To show that you're making progress.

At Wood for Trees we believe that compliance is not something to aspire to, but fundamentally business as usual. However, the way your charity approaches this can present a number of opportunities, from managing your supporters' privacy to increased engagement. Achieving growth through trust.

Trust can mean many things, from transparency of your CEO's remuneration package, to the percentage of funds being spent on good causes or who you are sharing data with? Controlling the 5W's of an individual's personal data, what (data is being collected), why (the purpose for which it was collected), who (has access to the data), where (the source data was captured) and when (the data captured) are pillars on which to build trust.

In May 2014, the World Economic Forum published 'Rethinking Personal Data: A New Lens for Strengthening Trust'. With global insights of the highest levels of leadership from industry, governments, civil society and academia, it articulates the value that a balanced and human-centred personal data ecosystem can create.

The key theme and priorities that emerged were the need for pragmatic and scalable approaches to personal data. Approaches that strengthen transparency, accountability and the empowerment of individuals. It highlighted the need for solutions and tools that answer fundamental questions - who has the data, where is the data and what is being done with it?

Given these findings, GDPR is the ideal starting point to develop a 'growth through trust' model – therefore organisations should embrace the new legislation, rather than viewing it as an upgrade to the Data Protection Act. Adopting an individual-centric model that gives the individual full control of their personal data is just one way to build trust.

The new regulation will undoubtedly be challenging and if not carefully managed will have a huge impact on current fundraising activities. However, smart organisations will also see the potential to build stronger relationships with their supporters, improve their reputation, benefit their cause and ultimately help their beneficiaries.

We hope you find your GDPR Checklist useful. If you'd like to find out more about our approach to privacy and consent, and how we can support you, please contact us.

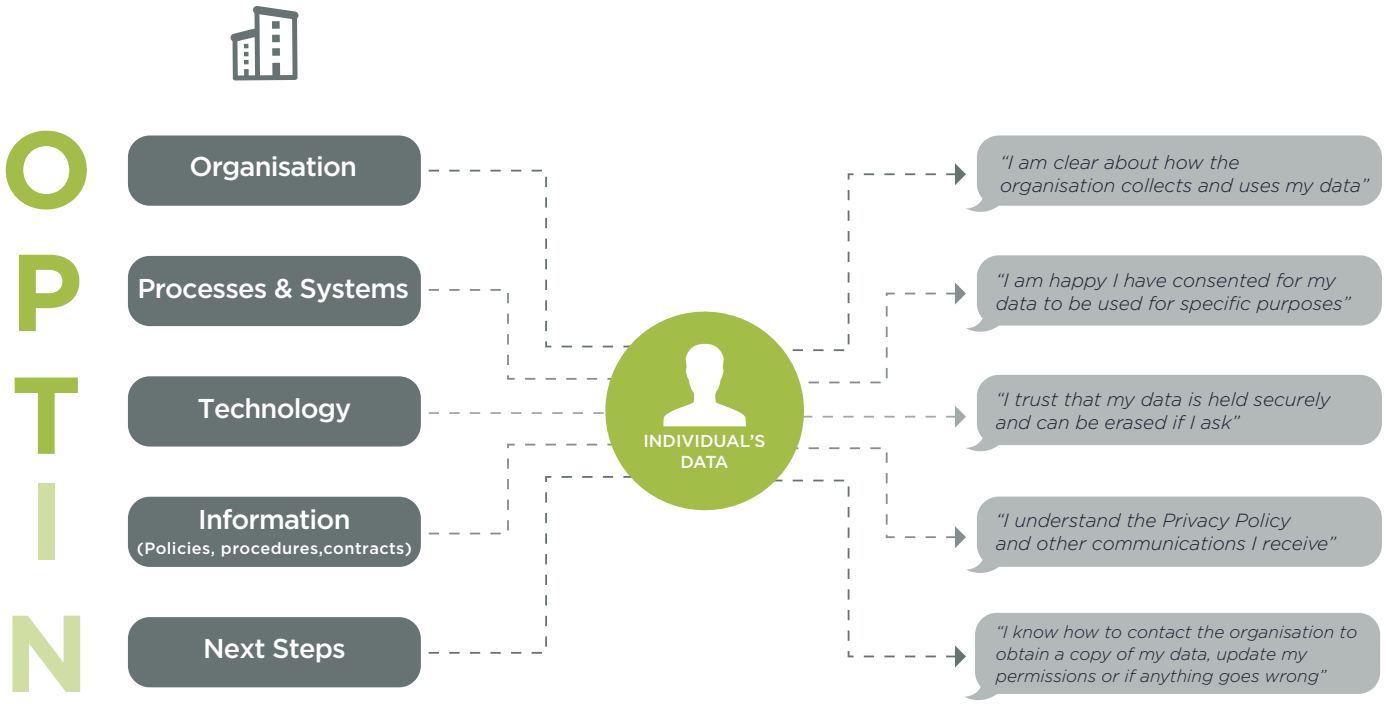
J Cromack
CEO, Wood for Trees
T: 01225 636 286
E: j.cromack@woodfortrees.net

GDPR Checklist

This checklist sets out activities you will need to consider – and act on – by the compliance deadline of 25th May 2018. Use this to help you identify what support you may need from across your organisation.

But please remember, this is for your guidance only and does not constitute legal advice. If in any doubt you should check with your organisation's compliance and legal advisors.

To make this more manageable we are using our OPT-IN acronym – below.



Continue to checklist >

Organisation

OPTIN

My board understands and supports GDPR.

☐ It is easy to think that this is just another regulation that you need to adhere to. It is not. It requires a new strategy. Risk needs to be managed. Your board needs to fully understand the impact and ensure resources are available to implement the changes.

We have checked we use plain English.

☐ Before you tick this box, just take a moment. Are your policies really easy to understand? Individuals need to be clear on what they are giving consent for and you need to ensure the language used is appropriate for your supporters, including children (if applicable). That means no legalese.

We have assessed and updated our Privacy Policy.

☐ Read our report 'Privacy Policies: How Does Yours Measure Up?' for the nine criteria that should be included in your Privacy Policy. We've reviewed the policies of 45 UK charities in light of recent rulings by the ICO and in preparation for GDPR. If you haven't got your copy yet, you can request it here: https://mylifedigital.leadpages.co/h-privacy-policies/

We have a Data Protection Officer.

☐ While you don't need to name a Data Protection Officer in your Privacy Policy, you do need a suitably knowledgeable person, or team of people, that individuals can contact regarding their personal data. If there is not someone with the expertise in the team, now is the time to train or recruit someone.

We know which departments will be impacted.

☐ No matter how tidy you think your systems and processes are you will need to impact assess all departments to identify how compliant their current processes are. Now you know who is affected you can plan appropriate action.

We have assessed the level of corporate risk.

☐ The recent announcement of the ICO's intent to fine a further 11 charities after the RSPCA and the British Heart Foundation highlight the ongoing risk for non-compliance. Under GDPR a two-tiered sanction will apply. Breaches of key provisions could lead to fines of up to €20 million or 4% of annual turnover. For less severe breaches, organisations could face a fine of up to €10 million or 2% of annual turnover, whichever is greater.

We understand how we communicate with our supporters.

☐ Under GDPR, consent to use a supporter's data to communicate for specific purposes will be required. You need to identify which purposes these are, whether you already have consent or whether you need to obtain it. There are certain communications – for instance, mandatory communications such as Direct Debit information – that do not need consent. Blanket consent no longer applies.

We have checked whether we are regulated by PECR.

☐ You have checked whether you are liable and need to be accountable to PECR. If you answer YES to any of these points, right, you need to ensure you're up to date for these regulations as well.

- Market by phone, email, text or fax?
- Use cookies or a similar technology on your website?
- Compile a telephone directory (or a similar public directory)

We have prioritised segments to convert to the right level of consent.

☐ Achieving consent from everyone on your database is an enormous task. Use this time to prioritise customers whose consent you need immediately so that you can minimise the impact on fundraising and service delivery.

We can be fully accountable.

☐ As an organisation you need to be fully accountable. Everyone has a part to play. Your people need to understand WHY the processes and procedures are in place. Compliance needs to be business as usual. Walk the talk. Don't just pay lip service; exercise the mindset to protect individuals' personal data.

Processes and Systems

OPT IN

We know the source of all data.

It is likely that data will be collected from multiple sources and may even be stored in numerous places. You need to map your inbound and outbound data flow.

We know what data we are holding.

Is your data categorised? Do you understand what sensitive data you hold? If not you need to pay attention to the new GDPR extended definition of sensitive data. Do you have specific consent to use this data? Do you need to collect and store it? If yes, for how long? GDPR stipulates that data should only be held as long as it is needed.

We are transparent about the use and sharing of data.

Supporters need to understand the purpose for which you have collected their data and whether you intend to share internally or externally with other organisations.

We can clearly demonstrate that we have consent to use this data.

Supporters need to be provided with a place to provide consent for the collection and use of their personal data for the specified purpose(s), or for sharing. They must also be able to easily change or withdraw these consents and have the ability to track the history of any amendments.

We have processes in place to delete data.

GDPR requires you to delete personal data when either you no longer need it, the purpose you collected it is no longer valid or when the supporter exercises their right to erasure. (There are noted exceptions to this clause).

We have systems in place to manage a data breach.

Organisational reputations can be destroyed by a data breach. GDPR requires that the authorities are informed and where there is a high risk to their rights and freedoms the affected individuals receive communication within 72 hours. There are some exclusions, such as if the data is encrypted.

We can comply with an individual's right to portability.

Portability of data is not a new concept but individuals have new rights. Individuals have the right to obtain their personal data and reuse it as they wish – as long as the information meets specific criteria. Organisations must be able to comply and send information in a commonly-used format within a month of it being requested.

Technology

We can provide details of all data electronically.

Supporters have the right to request a copy of the information you hold about them. You need to be sure that this data is accessible and can be readily extracted for the supporter.

All data is securely stored and safely encrypted.

As mentioned above, if data is encrypted and unintelligible to unauthorised persons, your organisation could potentially be exempt from the 72-hour requirement to notify supporters of a data breach. Of course, you would still have to notify the relevant authorities.

We can fulfil the 'right to be forgotten'.

You need to demonstrate the capability to completely erase all personal information, from every department, spreadsheet and system. Under GDPR, an individual has the right to be forgotten. You also need to inform any external parties, where this personal data has been shared to do the same.

All new technology has privacy by design built-in.

Whether you are upgrading existing systems, or specifying new systems, privacy should be built in by design. Then you are sure that the privacy of your donors, supporters, volunteers and service users is assured.

Information and rights of access

We have updated all our permission statements and they are ready for GDPR.

Your permission statements and Privacy Policies need to be specific and relevant to your organisation. You will need to seek explicit consent and only collect data for legitimate purposes.

Individuals can easily find out what information we hold on them.

This is the acid test on compliance. Can you easily tell an individual what information you hold, how it was obtained, when it was consented and, if they request it, that you can delete their personal data from **all** your systems.

We can verify individual's ages and identify children for specific consent.

The regulations raise the age of consent for collecting an individual's data from 13 to 16 years old. If your charity collects data from children, you will need a process in place to verify an individual's age, identify children and seek parental or guardian consent for use of their data.

We have developed template responses.

Use the time before May 2018 to create template responses to individual's requests for example a subject access request. This serves two purposes. To prepare your team(s) to ensure they know what to send, and that all of the supporters' requirements are met.

We know what additional information needs to be collected to adhere to GDPR.

Because of DPA there will already be consent in place for some – if not all – data. However, there will be gaps. Gaps could include being able to erase data, timestamp when consent was obtained, or obtain specific consent for particular purposes.

Next Steps

OPT IN

We have tested an individual's experience when requesting consent.

Many charities are concerned about the impact on supporters when requesting consent. Use this time to trial new approaches. To monitor impact and identify how to make consent business as usual in engaging and building trust with your supporters.

Individuals can access their own data and update their preferences.

GDPR is citizen centric. This puts the supporter in control of how their data is used. Where supporters can give or withdraw permission easily. Where transparency is absolute.

We can put it right when we've got it wrong.

If an individual knows that information you have is incorrect, you must be able to update their information, and record additional information, if that is required. It's formally called the right to rectification.

We can restrict profiling.

GDPR gives supporters significant rights to object to profiling processes. This is in response to the proliferation of new technologies which allows for advanced data analytics. This is a hotly contested aspect of the new regulations, and one that can have the most impact on fundraising practices and income generation. We will be looking in more depth at this subject. To find out more email j.cromack@woodfortrees.net

Our marketing, fundraising and other departments that use data are fully aware of policies, procedures and the new GDPR regulations.

Training can easily be overlooked but ignorance is no defence. Every person who has access to data – and / or who uses data as part of their role – needs to be fully aware of the new legislation, the policies and procedures of your own organisation and that consent is a new route to engagement with your supporters and service users.

About Wood for Trees

Rethinking Personal Data. We can help you:

- improve the efficiency, fundraising and performance through Wood for Trees,
- comply with existing legislation and GDPR regarding the collection of personal data,
- make informed insights from informed consent from your supporters to improve outcomes.

You can reach us using the contact details below.

www.woodfortrees.net

T: 01225 636 286

E: j.cromack@woodfortrees.net

Wood for Trees Ltd, Reg Office: Citizen House, Crescent Office Park, Clarks Way, Rush Hill, Bath, BA2 2AF

wood for trees