|  |  |
| --- | --- |
|  |  |
| BVSC’s GDPR ‘TO DO’ LIST | |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Priority** | **Due Date** | **What** | **Who** | **In Progress** | **Done** | | 1. | Beginning of May | **Raise Awareness – that GDPR is coming!**  Ensure staff, volunteers and trustees know what the new legislation is about  Ensure staff and volunteers know what their responsibilities will be  Ensure you have the knowledge to update your policies and procedures  Organise external training for managers/those with responsibility for overseeing GDPR  Organise internal training for staff and volunteers – anyone involved with processing data  You may use the [video clips](https://www.bvsc.co.uk/gdpr-how-videos) to go through the various elements as a training resource  A good start is to run through the [ICO principles of GDPR](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/) with staff and volunteers and there is a great selection of material [to help remind your staff and volunteers of their responsibilities](https://ico.org.uk/media/for-organisations/think-privacy/2563/ico-think-privacy-toolkit-edgy-type-charities.pdf) | Manager, Trustees or those responsible for implementation |  |  | | 2. | Mid-May | **Data Audit**  Record of all the data you hold  Decide (as a team) if it is necessary to collect it.  Decide how is processed and why  Clarify who processes the data  Be clear about where the data comes from  Know who you share it with and why  There are 3 audit templates of varying complexity – choose a format that suits your organisation and size.  [Information Audit Template (1)](https://www.bvsc.co.uk/information-audit-template)  [Simple Information Audit Template](https://www.bvsc.co.uk/simple-information-audit-template)  [Data Audit template](https://www.bvsc.co.uk/data-audit-template) | This is normally a whole team task. Everyone in your organisation that collects data should contribute |  |  | | 3. | Mid-May | **Create or Update Privacy Notices**  Create a simple and plain English Privacy Notice – remember your service users need to understand it easily  Ensure it is easily accessible and always available where data is collected  Explain why you need the data, what you will do with it, who you will share it with.  It needs to include:   * Lawful basis for processing * Retention periods * How the individual can refer to ICO   There are several templates and examples of Privacy notices from the very detailed to very simple. It doesn’t matter which you use as long as it is proportionate, easy to understand and compliant.  [Good example of charity Privacy Notice](http://www.cancerresearchuk.org/privacy-statement)  [Privacy notice for employees](https://www.bvsc.co.uk/privacy-notice-employees)  [Privacy notice for sending emails](https://www.bvsc.co.uk/privacy-notice-sending-emails) | Person or Trustee responsible for GDPR compliance |  |  | | 4. | By mid-May | **Lawful Basis**  You must identify the lawful basis for your processing activity – this must be approved by your Management Committee/Trustee Board  Document it  Update your privacy notices  **See Appendix 1. Lawful Basis** | Person or Trustee responsible for GDPR compliance |  |  | | 5. | By mid-May | **Data Privacy by Design**  You should adopt a ‘data privacy by design’ approach to developing existing or new services which include data processing – this means that compliance is there from the start, not an after-thought or bolted on. Ensure staff understand the importance of protecting the organisations reputation. Your biggest risk is from service users making a complaint! Consider a process your organisation can use to show how data privacy has been considered for each service/project | Whole team |  |  | | 6. | By 25th May | **Subject Access Requests**  You must respond within 30 days  They are free of charge  They can be refused – but only if they are ‘manifestly unfounded’ or ‘excessive’  If you refuse a request, tell the individual why and that they have the right to complain to Trustee Board or ICO  Have a plan for dealing with Access Requests from May 25th  **See Appendix 2. SARs** | Person or Trustee responsible for GDPR compliance |  |  | | 7. | By 25th May | **Data Protection Impact Assessment (DPIA)**  When organisations undertake data processing with a ‘high risk of adverse effects’ on individuals a DPIA should be made. A [checklist](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) will help you decide if a DPIA will apply to your organisation. | Person or Trustee responsible for GDPR compliance |  |  | | 8. | By 25th May | **Data Breaches**  Policies and procedures to be in place to detect, report and investigate a personal data breach  Assess the types of personal data you hold and document where you would be required to notify if a breach occurred  Policies and procedures in place to manage data breaches  \*Failure to report to breach when required to do so could result in a fine as well as a fine for the breach itself.  **See Appendix 3. Data breaches** |  |  |  | | 9. | By 25th May | **Third party suppliers/partners**  As an organisation, it is your responsibility to ensure any third parties you work with that have access to your data are GDPR compliant. This might be the people who host your website or CRM, your IT support, your payroll, Dropbox or WordPress etc.– anyone that can either control or process data on your behalf. It is a good idea to make a list of all organisations that have access to your data and record their individual response to GDPR compliance request.  For example, our payroll company is BrightHR and this is [their response](https://www.brightpay.co.uk/docs/17-18/gdpr/gdpr-and-brightpay/) to our enquiry re compliance. This tells us that they are aware of GDPR, have made key changes and are still working towards full compliance. |  |  |  | | 10. | By 25th May | **Do you need a Data Protection Officer?**  You need one if:  You carry out regular and systematic monitoring of individuals on a **large scale**  You carry out **large scale** processing of special categories of data, such as health records, or information about criminal convictions  ‘Large Scale’ at the moment is not particularly well defined.  If you do need a Data Protection officer:   * Can be a part time role * Organisations can share DPO’s * The DPO will have responsibility for compliance * The DPO will have access and influence at Board level * The DPO **will not** be involved in data processing activities (ideally an external role)   This is very unlikely to apply to the majority of voluntary and community groups in Bexley but may apply to large or regional charities. | Person or Trustee responsible for GDPR compliance |  |  | | 11. | By 25th May | **Reviewing your existing data**  Data you currently hold – after 25th May you will need to demonstrate that consent for existing data was gained in a GDPR compliant manner and is used for the purpose it was given.  For many/most organisations this will mean seeking consent in a GDPR compliant way from existing users/beneficiaries. | Whole team |  |  | | 12. | By 25th May | **Finally! Get ready to work with individuals**  Have all your policies and procedures in place  Make sure all your members receive communications from you because they have explicitly consented or because you have a legitimate interest in communicating with them.  Know about subject access requests (see Step 6)  Be able and willing to share, update, amend or delete any data at any time (according to policies/lawful basis agreed)  What about children? **Appendix 4**  Make sure your charity’s Data Protection Policy follows GDPR guidelines – a good example is [here](https://drive.google.com/file/d/1qdP0w_jIx6CgrZuz7VfPAxPVGQB_88jd/view)  Further guidance and FAQ’s **Appendix 5**  **USE THE ICO HELPLINE FOR ALL QUERIES 0303 123 1113** | Whole team |  |  | |  |  |  |  |  |  | | |
|  | Further reading: [ICO guide for charities](https://ico.org.uk/for-organisations/charity/)  [Charities Finance Group - GDPR guide for charities](http://www.cfg.org.uk/resources/Publications/~/media/Files/Resources/CFDG%20Publications/CFG266_GDPR.pdf)  [Fundraising & GDPR - a guide](http://2040training.co.uk/wp-content/uploads/2017/03/Fundraising-DP-guide.pdf)  [Institute of Fundraising GDPR pack](https://www.institute-of-fundraising.org.uk/guidance/research/get-ready-for-gdpr/)  [10 step action plan Infographic](https://www.bvsc.co.uk/gdpr-10-step-action-plan) [GDPR at a glance Infographic](https://www.bvsc.co.uk/gdpr-glance) |

BVSC’s GDPR ‘TO DO’ LIST – APPENDIX 1

**Lawful Basis for Processing Data**

There are 6 lawful bases for the collection of personal data:

* Consent -the individual gives clear consent for you to collect data
* Legitimate interest -data is for the legitimate interest of your organisation or third party
* Contract -when you have a contract with the individual eg an employee
* Legal obligation -when you need to collect data to comply with the law eg HMRC
* Vital interests -when data is needed to save someone’s life eg a hospital setting
* Public task -if you are a public body eg a local authority

We will look in some detail at Consent and Legitimate interest as it is likely that most voluntary sector organisations will be using either one of these as their lawful basis to collect data. You should investigate the other four bases in more detail with specialist advice if you feel they may apply to your organisation or the type of service you deliver.

**Consent**

* Consent must be freely given, specific, informed and unambiguous.
* There must be a positive opt-in; consent can’t be assumed from silence, pre-ticked boxes or inactivity.
* It must be separate from other terms and conditions
* There must be a simple way for people to withdraw consent (as simple as it was to consent eg an ‘Unsubscribe’ button)
* Consent must be recorded and available for inspection
* If you have a current members/service users and you did not receive fully compliant GDPR consent from those individuals, they have to be contacted again for consent. This should be done before 25th May or as soon as possible after in order to ensure you are communicating in compliance with GDPR

[ICO guidance and checklist on consent](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/)

[Example form Consent from members](https://docs.google.com/forms/d/e/1FAIpQLSf9arjJ_9fFV_WOBvLpdIaV2hRa277800ox0jhQV49-sVDlAw/viewform)

**Legitimate interest**

* The most lawful basis for processing – but don’t assume it will always be appropriate!
* It is likely to be appropriate if you can show; how you use people’s data is proportionate, has minimal privacy impact, compelling justification for the processing, and people are not likely to object if you explained it to them.
* The legitimate interests can be your own or the interests of a third party (eg for societal benefits)
* The processing must be necessary. If you can achieve the same result in a less intrusive way, legitimate interest will not apply
* Would the individual reasonably expect the processing if you explained it to them?
* Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance
* You must include details of your legitimate interests in your privacy information

[ICO checklist and guidance on Legitimate Interest](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/)

**\*Minute the decision made at Trustee Board level on all decisions re GDPR eg your legal basis for processing data**

BVSC’s GDPR ‘TO DO’ LIST - APPENDIX 2

**Subject Access Requirements**

The GDPR regulations includes the following rights for individuals:

* The right to be informed
* The right of access
* The right to rectification
* The right to erasure
* The right to restrict processing
* The right to data portability
* The right to object
* The right not to be subjected to automated decision-making including profiling

What this means for organisations, is that your staff, volunteers or service users have the right to see the information you hold about them, to ask for it to be amended or deleted or for it to be processed in certain ways only.

Check your procedures and work out how you would manage someone asking for their data to be deleted or how you would locate the data that someone wanted to see before it was deleted. Who will make the decision about deletion? It is likely you will need to make some changes to ensure you can provide all of the relevant personal data easily, quickly and in a machine readable form. Have a trial run – choose a user or member of staff and see how quickly you can provide all information about them and what is available. Any issues can be your starting point to review practices.

The information requested must be provided within one month and must be free of charge.

Actions to prepare for SARs:

* Design a template response letter so you can ensure that all requirements are complied with
* Develop a policy/procedure for dealing with SARs and ensure they take into account new timescales
* Ensure employees and volunteers are trained to recognise when a beneficiary has made a SAR and knows how this is to be dealt with
* Think about how data is stored and how easy it would be to retrieve it (including emails, hard copy letters, texts) and remember the subject is only allowed to see information relating to them in a letter or email, not the whole letter or email.

[ICO guidance and checklist SAR](https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/)

[10 top tips for responding to a SAR](https://www.kingsleynapley.co.uk/insights/blogs/employment-law-blog/top-10-tips-for-responding-to-a-subject-access-request)

[Sample SAR Policy](https://www.bvsc.co.uk/sample-sar-policy)

BVSC’s GDPR ‘TO DO’ LIST – APPENDIX 3

**Data Breaches**

What is a data protection breach?

*“A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.” ICO*

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

You have 72 hours to report a data breach **unless** you have breached people’s own login details eg password which will leave some people very vulnerable, for instance, those that use the same password for multiple sites. In this case you should aim to report to both the ICO and the individual within 24 hours so they can change passwords etc.

The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases to individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or effected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Make sure you add Data Protection breaches to your Risk Register

Make sure are trained and supported to identify a data breach

[ICO guidance on data breach](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/)

BVSC’s GDPR ‘TO DO’ LIST – APPENDIX 4

**Children**

You should start thinking now about whether you need to put systems in place to verify individuals ages and to obtain parental or guardian consent for any data processing activity.

Review any privacy information given to children and ensure it is appropriate for a child

Make sure you keep up to date with relevant codes of conduct which might affect any associations or groups your charity might participate in.

GDPR will introduce special protection for children’s personal data, in particular commercial internet services such as social networking. Organisations which offer online services to children and rely on consent to collect information will be directly affected and must ensure language is tailored for the target audience. Processing of data related to children is noted to carry certain risks, and further restrictions may be imposed as a result of codes of conduct.

*Under Article 8(2) GDPR, charities will need to make “reasonable efforts” to verify that consent has been given or authorised by the holder of parental responsibility. However, charities will not need to seek the consent of parental figures when the processing is related to preventive or counselling services offered directly to the child. Children “may be less aware of the risks, consequences and safeguards” of handing over their personal data.” Crowe Clark Whitehill (Guide to GDPR)*

**Only children over 13 years are able to give their own consent.** Please keep checking this is there has been talk about this age of consent being changed to 16 years old. At the time of writing (April 2018) it is 13 years old.

You must write clean and age-appropriate Privacy Notices for children.

[ICO guide to GDPR and children](https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf)

BVSC’s GDPR ‘TO DO’ LIST – APPENDIX 5

**Top five tips**

Here are our top five of data protection tips for small and medium sized charities and third sector organisations:

**Tell people what you are doing with their data**  
People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

**Make sure your staff are adequately trained**   
New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.

**Use strong passwords**  
There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower-case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.

**Encrypt all portable devices**  
Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

**Only keep people’s information for as long as necessary**  
Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

**What are PECRs?**

Privacy and Electronic Communications Regulations (PECR) are still in effect and apply to direct marketing sent by electronic communications eg email and text. Under that, you cannot send unsolicited electronic direct marketing to individual subscribers (including sole traders and partnerships) without their prior consent. The PECR is currently being amended and it is expected that the amended regulations will come into force some time in 2019 and will be brought into line with GDPR. Under the new rules, corporate subscribers will be as protected as individual subscribers.

More information on PECR [*https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/*](https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/)

**Do charities need to register with ICO?**

No. The ICO registration team have said that if, in your constitution it clearly states, "we are a not for profit organisation." it is likely that you do not have to register with the ICO. However, whilst this wording would mean that you are exempt from registering, you still need to abide with GDPR e.g. you would still need to report breaches to the ICO. Please contact the ICO if you have more specific questions about this.

**Guidance on photography and sharing images of children**

NSPCC have produced this [helpful guide](https://www.nspcc.org.uk/preventing-abuse/safeguarding/photography-sharing-images-guidance/)

A simple guide to taking and displaying photos and use of CCTV is [here](https://www.bvsc.co.uk/guidance-using-images-cctv)

**How long do we have to keep data for?**

There are some hard and fast rules about different types of data and how long you must keep them for, however, for data that does not have a legal time limit for keeping, it is up to you as an organisation to not keep anything longer than necessary and to have a reasonable justification for information you do decide to keep. Please contact ICO if you are not sure about any aspect of keeping data for a set period of time.

This is a [useful template](https://www.bvsc.co.uk/document-retention-policy) for Data Retention records that you can use