General Data Protection Regulation (GDPR) Action Plan

Contents

Information for Arts Organisations

You need to be ready by **25 May 2018**

GDPR impacts on fundraising, finance, marketing, education work- anything involving people **(the data subject),** where you as an organisation **(the data controller)** collect, hold and use personal information about them **(data processing).** This could include names, emails, dates of birth, addresses- anything that could identify them **(personal data)**. GDPR also applies to organisations that just use data, don't own or collect it **(data processors),** for example external payroll providers who just use data you provide to them.

GDPR uses a lot of the same principles as current data protection law but there is a greater emphasis on transparency (what data you collect and why), privacy (the rights on the individual) and accountability (showing how you are compliant).

When can you process data?

You need to have a reason to collect, hold and use data. Reasons relevant to arts organisations under GDPR are:

1. Contract: it's necessary to enter into or deliver a contract e.g. a customer gives you their address because they want you to post their ticket to them or you hold employee data so you can pay them.

2. Legal obligation: the processing is necessary for you to comply with the law e.g. gift aid records

3. Legitimate interests: the processing is necessary for legitimate business interests e.g. telling an existing audience member about a new, similar event that is coming up or holding information about a participant so that you can provide a safe and appropriate service to them.

4. Consent: the individual has given clear consent to you e.g. opting in to a mailing list

You need to have at least one of these reasons to process data.

Consent, Legitimate Interest, Marketing and Fundraising

If you want to use send direct marketing to someone (promoting a show, sending information about a fundraising campaign, or sending information about your organisation's aims) then you need to have clear consent or have carried out an assessment and can clearly demonstrate legitimate interest.

Consent

Consent must be freely given by a statement or clear affirmative action e.g. asking to be added to a mailing list, ticking a box on a website, filling in a sign up form. NOT pre-ticked boxes or opt-out.

It must be as easy to withdraw consent as it was to give consent e.g. unsubscribe options on emails, information on your website about how to unsubscribe.

You need to keep records of how and when consent was given. If you use mailchimp you can add a field to your lists which says where and how consent was given if you're entering addresses manually e.g. "emailed to ask to be updated 26/01/18" or "left email address for mailing list after Spring Festival 2018 event". It autocompletes on this feature too which is useful if you enter lots of people manually who have signed up in similar ways.

Information about what the personal data will be used for must be unambiguous, specific and easy to understand.

Where possible give granular options e.g. let people choose if they want information about fundraising, specific projects, shows, exhibitions and what methods they want to be contacted by.

If you are gaining consent for sharing information you need to be as specific as possible e.g. not just saying "other relevant organisations" but naming actual organisations and saying when and how the data will be shared and used.

You need to keep consent under review. This is interpreted in different ways but could include asking mailing list subscribers to re-subscribe periodically, sending updates and unsubscribe options to remind people what they signed up to and regularly cleaning your database from subscribers who never open an email from you.

Legitimate Interest

In marketing terms, get consent where you can. If not then you could potentially use legitimate interest. You need to assess whether there is a legitimate interest for you as an organisation to contact someone and balance this against their individual right to privacy.

Post and 'phone: Direct marketing is a legitimate business interest and you can send information by post or make live (not automated) 'phone calls to people (as long as you check the Telephone Preference Service). You need to have a clear case and this needs to be balanced with the individual's right to privacy. e.g.

Yes: posting someone a newsletter about similar events because they have attended events in the past
No: making numerous ‘phone calls to someone about fundraising because they bought a ticket once 10 years ago and left their ‘phone number.

The law regarding ‘phone may be changing in future to be the same as email so where possible move towards using consent rather than legitimate interest.

Email and SMS

When you do not have consent, you cannot send direct marketing via email or SMS.

However, there is an exception to this rule. Known as the 'soft opt-in' it applies if the following conditions are met;

- where you've obtained a person's details in the course of a sale or negotiations for a sale of a product or service;
- where the messages are only marketing similar products or services; and
- where the person is given a simple opportunity to refuse marketing when their details are collected, and if they don't opt out at this point, are given a simple way to do so in future messages.

When you send an electronic marketing message, you must tell the recipient who you are and provide a valid contact address.

If you are using legitimate interest for direct marketing and the customer chooses to unsubscribe or asks you to stop you must do so immediately.

In practice this means:

Yes: sending an email about a dance show to previous bookers of a dance show at the same venue, including an unsubscribe link. Your booking page would carry information about marketing and how to opt out at point of booking.

No: sending an email about fundraising to someone who left their email at an exhibition because they’d left their hat behind.

No: sending an email to someone about fundraising when they had left their email address on a sign up sheet for information about circus classes.

Children and Young People

If you are processing data of children and young people then you need their guardian’s permission. Any information presented to children and young people about their data needs to be in language which they can understand.

Breaches

It will be mandatory to report a personal data breach to the ICO within 72 hours if it's likely to result in a risk to people's rights and freedoms. So if it's unlikely that there's a risk to people's rights and freedoms from the breach, you don't need to report.

High risk situations are likely to include the potential of people suffering significant detrimental effect – for example, discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage. You may also need to make a serious incident report to the Charities Commission if you're a charity as you have reported to a third party regulator.

Checklist

- ✓ **Carry out an audit** of what data you process, how, why, how long for and whether it is held securely. Create an action list to ensure all of the data you process is done so in a compliant way. (Audit template attached- sheet 1)
- ✓ **Audit your third party processors**- who do you share data with? Do you know they are GDPR compliant? (Audit template attached- sheet 2)
- ✓ **Check and update your consent statements and privacy statements** on your website, mailing list and paper documentation used to collect data e.g. sign up forms. Statements need to include:
    - What the data is being collected for
    - How it will be used
    - Where relevant, options for opting in and choosing what information is received and through what channels
    - How the data subject can contact you to update or request the removal of their data

Look at bigger charities websites for examples that meet these criteria, using the ones you feel are clearest to you as a member of the public as a starting point for your own organisation.

- ✓ **Set up a process for reviewing your data processes** and carrying out audits to ensure that appropriate steps are being followed. This could be reviewing your data audit annually, including briefings in all staff inductions, making data protection an agenda item in some team meetings and carrying out checks to make sure that procedures are being correctly followed for your higher risk data processing e.g. regarding children and young people or where you are carrying out

marketing and fundraising activity or holding sensitive information e.g. around DBS checks.

- ✓ **Appoint someone in your organisation to lead on data protection** and ensure that all staff are briefed so they know
  - What data you hold and why
  - How to ask for and record consent where needed
  - How to store data securely
  - What you have permission to use the data you work with for and that they should not use it in any other ways
  - What to do if someone wants their data to be removed from mailing lists etc
  - Who to talk to if they think they may have made a mistake regarding using data or keeping it secure
  - That any data they record about someone can be subject to a freedom of information request and so they need to think about their choice of words regarding data subjects in emails etc.
- ✓ **Create a data policy** which includes:
  - What your procedures are for data processing (from your audit)
  - Who is responsible for leading on data protection in your organisation and how staff are trained and briefed (ICO suggest on induction and then every 2 years)
  - How you record, review and check compliance with your procedures
  - What to do in the event of a breach
  - How you will deal with a request from an individual to see the data you hold on them or delete all data you hold on them

Registration and fees

Under GDPR there will no longer be a requirement to register with the ICO as a data controller. There will however be a fee to pay to the ICO for all organisations that use data. The tier 1 rate which is for small organisations and charities is £40 (which most small arts organisations fall under). More information is available here: https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf

and you can register here: https://ico.org.uk/for-organisations/register/

Further Resources

Information Commissioners Office https://ico.org.uk/for-organisations/

GDPR helpline for small organisations 0303 123 1113

GDPR training session slides from the Directory of Social Change are available here: https://www.dsc.org.uk/gdpr-need-know/

GDPR essentials for Fundraising Organisations https://www.institute-of-fundraising.org.uk/library/gdpr-the-essentials-for-fundraising-organisations/iof-gdpr-essentials-report-final-v1.pdf

This checklist is useful for marketing: https://ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf