General Data Protection Regulation (GDPR) will apply from 25 May 2018
It's not all about consent!

BAFA general guidance and comments. For in-depth information please refer to the ICO website

Which comes first?
Your new/updated Privacy Policy (your website will have something on it already about Cookies even if you don't have anything else) or GDPR compliance?

Well, they are interleaved. Your new/updated Privacy Policy explains how you are complying with the new GDPR legislation. So don't go emailing your contacts list asking for consent to continue emailing them before you have written your new/updated Privacy Policy – that is where you point people. And – you will probably discover that you don't need to email your contacts list anyway.

Read on ….

1: GDPR applies to all
The GDPR applies to all companies worldwide that process the **personal data** of European Union (EU) citizens. The GDPR considers any data that can be used to identify an individual as personal data. It includes, for the first time, things such as genetic, mental, cultural, economic or social information.

And it covers what you use personal data for – and – how you gather it and store it.

BAFA top tip: even when the UK leaves Europe these regulations will currently still apply.

2: Action plan:
The requirements can be divided into four steps:
A: Audit
B: Consent
C: Storage
D: Rights

A: Audit
Make a list of all the physical and digital places you store data. Do you have an ancient box of paper feedback forms under someone's desk/bed/table each with a personal email address on? Do any of your committee or board have personal data on their own computers or other devices?

Here is the list that BAFA made:

External websites	**BAFA email accounts**
Eventbrite	Office 365
MailChimp	Gmail
Smart Survey	Yahoo
TicketSource	
Dropbox	**Databases**
Survey Monkey	Members
Doodle	Contacts
Facebook	

Twitter	**BAFA websites**
Instagram	www.artsfestivals.co.uk
LinkedIn	Conference website
Sage	Student conference website
Flickr	
TweetDeck	**Devices**
Hootsuite	BAFA laptop no1
YouTube	BAFA laptop no2

Once you have made your audit list, work your way through each item on it to interrogate:

- If you need to keep that data in that format – simplification makes life so much easier
- To plan how you are going to ensure compliance with GDPR and that includes third party accounts such as MailChimp or Eventbrite
- And to wrap up all this activity in easy to read language in your new/updated Privacy Policy.

BAFA top tip: You must have a valid lawful basis in order to process personal data. Consider what this is and include it in your new/revised Privacy Policy.

B: Consent

"A freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity."

Existing lists do not need to be 're-consented'

Scrutinise the reasons you told people why you wanted their personal details. If these remain valid – **you do not need to ask for their consent a second time**. You may choose to ask for 'additional' consent, but do not risk decimating your precious data lists unnecessarily.

- Inform people what you are doing in simple language
- Inform at time of consent of right to withdraw
- Inform how to complain/exercise rights.

This means that consent must be:

- **Unbundled** – separate from other terms and conditions
- **Active opt-in** – no pre-ticked boxes or implied consent
- **Granular** – applied to separate processing and purposes
- **Verifiable** – records must be kept to prove what consent was provided for
- **Easy to withdraw** – just as easy as it was to provide
- **Refreshed** – valid consent does not last forever.

BAFA top tip: '**Soft Opt-In' explained**

There is an exception called the 'soft opt-in'. This means that consent is not required if you are sending a marketing message about similar products and services to your customers/clients or those you have negotiated with to provide products or services, as long as:

- You give them the opportunity to opt-out when you receive their contact information; and
- You give them the opportunity to opt-out when you send them subsequent messages.

This processing is not based on consent, but rather the 'Legitimate Interests' processing condition and can only be relied up on by the organisation that collected the contact details, not third parties. Ensure this is written into your new/updated Privacy Policy.

And another top tip: **Consent cannot be a condition of service**, but it can be incentivised with 'non-essential' tasks such as signing up to your Wi-Fi, but this must not be obligatory.

And a final top tip: **Take care not to undo one consent with another**. Make sure each person/department shares consent wording. This is the 'Granular' aspect referred to in the bullet points above, but there is no benefit in offering a long list of options, keep it simple.

The ICO States:
You can rely on legitimate interests for marketing activities if you can show the way you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object to what you are doing

3: Storage
Where do you store your data? On your laptop/desktop/cloud?
Consider encrypting your laptop, otherwise if lost or stolen, the password could be hacked and the data on it can be transferred to another machine by removing the hard drive.
On a desktop, a server, in the Cloud, in Dropbox, etc? All of these places need to be scrutinised and the risk considered and new security put in place if necessary.

Third parties: Where do they store your data?
All of the companies on BAFA's list in section 2 now have privacy statements on their websites and/or reference GDPR. It is the responsibility of everyone to familiarise themselves with these statements and take an informed decision to continue with their use – or otherwise.

How long can you store the data?
There is no regulation that stipulates length, but the guidance stipulates 'no longer than necessary for the purpose'. Decide what this is and include it in your Privacy Policy.

BAFA top tip: Privacy Shield is a protocol that many companies who store EU data outside of the EU are signed up to, especially those with USA connections. This places strong data protection obligations on companies receiving personal data from the EU. MailChimp is an example of a company that is signed up to this protocol.

4: Rights
- 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 object

BAFA top tip: Use these 6 points as a tick list to ensure each is covered in your new/updated Privacy Policy.

And some other relevant issues:

5: Business data

What constitutes 'personal data'?
The rules about prior consent don't apply in quite the same way to business or work emails and this includes a personal email that is used in the context of work/business purposes. This is also where PECR regulations come in. PECR existed well before GDPR and you should already be familiar with this protocol, though it largely is designed to restrict unsolicited nuisance marketing.

The GDPR does not replace PECR – although it has amended the definition of consent. You need to comply with both GDPR and PECR for your business to business marketing.

The EU is in the process of replacing the current e-privacy law with a new ePrivacy Regulation (ePR). However, the new ePR is yet to be agreed. The existing PECR rules continue to apply (with the new GDPR definition of consent) until the new ePR is finalised.

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- Marketing calls, emails, texts and faxes
- Cookies (and similar technologies)
- Keeping communications services secure
- Customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Guide to electronic and telephone marketing

What does that mean in practical terms? Only that the rules about prior consent to e-mail marketing don't apply – which is why we all receive so many unsolicited communications to our work in boxes, but not to our personal e-mail addresses (and why there will continue to be a thriving trade of e-mail addresses harvested from LinkedIn after GDPR comes into effect).

You still have to satisfy a condition for processing in order to be able to use that e-mail address. That condition might well be 'Legitimate Interest' but if that is going to be the case then you will need to perform a Legitimate Interest Assessment and document the fact that that's the condition you are relying on in your new/revised Privacy Policy.

All of the other rules about processing, storing personal data apply to 'work' e-mail addresses in the same way as they apply to 'personal' ones (so they are to be kept securely, not used for purposes that the data subject was not originally informed of and couldn't have foreseen, are disclosable in response to a Subject Access Request, etc etc).

BAFA top tip: So if, like BAFA, you need to contact someone for a professional reason you can search for their email online, or use another method to source the contact details be they phone, address or email, and use those details to contact that person, but - include a paragraph about your 'Legitimate Interest' approach in your new/amended Privacy Policy and include how you will treat the information you retain.

6: Data Protection Officer (DPO)?
1. Is it mandatory?
2. Is it desirable?
3. Irrespective: take ownership of 'data protection' issues more generally and delegate responsibility.

Most BAFA Members will not be required to appoint a DPO (see rules below), but it is good practise to have one member of staff who takes responsibility for this. In a small team it has been suggested printing out your Privacy Policy and have everyone physically sign it. This can help focus people's minds on the importance of this. Your designated member of staff (rotate this role so everyone becomes really well acquainted) should undertake to be responsible for:

1. Knowledge of what personal data you hold and where/how you hold it – knowledge of key risks
2. Responsibility for co-ordinating responses to individuals (and the ICO if they come calling)
3. General staff awareness
4. Review and audit of new processes
5. Regular review of processes and maintenance of reporting documentation.

Rules for appointing a DPO:

- *You are a public authority (except for courts acting in their judicial capacity)*
- *Your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking)*
- *Your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.*

BAFA top tip: Are you registered under the Data Protection Act? Check if you should be here. Cost for charities is £35, but check as you may not need to register.

7: Privacy Policy

This is BAFA's key statement

- We respect your contact data
- We will store it securely
- We will never share it with anyone else
- We will delete it when you ask us to
- We won't contact you if you ask us not to.

And please read and use the BAFA updated Privacy Policy.

BAFA top tip: Update your Privacy Policy as regularly as you feel you need to and date it accordingly. As your knowledge and awareness of how you handle personal data grows then reflect that in your Privacy Policy. Don't be afraid of stating the obvious. Use easy to understand language. Set up Google Alert for keywords, read the specialist press, sign up for ICO updates - and above all keep informed.

This summary is provided for guidance only and includes information that to the best of BAFA's knowledge is correct as of 15 May 2018. *Please do not rely on this alone* and refer to the ICO website for full details.

Please contact BAFA HQ if you think something here is not correct, you can add to this knowledge, or you have any specific queries which we will do our very best to help you with.

BAFA HQ
info@artsfestivals.co.uk