General Data Protection Regulation – The Fringe Society's Guide for Venues and Companies

Contents

What is GDPR?

General Data Protection Regulation (GDPR) replaces the previous Data Protection Act, and outlines a new legal framework for the management, processing and usage of personal data.

GDPR was adopted by both the European Parliament and the European Council in April 2016; click for the regulation and directive.

GDPR came into force on 25 May 2018. It will be enforced by the Information Commissioner's Office who will manage reporting, compliance and any enforcement.

This change in the law means we are changing the way we handle and process customer data, including how this is shared with third parties, such as venues and companies.

Please note, this guide is intended to help and does not constitute legal advice. Please ensure you and your organisation take appropriate advice before taking action.

What data is affected?

Both personal data and sensitive data are covered by GDPR. Personal data, a complex category of information, broadly means a piece of information that can be used to identify a person; such as a name, address, IP address. Sensitive personal data encompasses genetic data, information about religious and political views, sexual orientation, and more.

Processing data

There are six lawful basis for processing data under GDPR:

1) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
2) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3) Legal obligation: the processing is necessary for you to comply with the law.
4) Vital interests: the processing is necessary to protect someone's life.
5) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

You should familiarise yourself with requirements of your organisation to review the data you hold and the grounds on which you can process this. You can download a very useful guide here which can help you get to grips with your GDPR requirements.

Legitimate interest Vs consent

You should by now have a clear understanding of the data you hold and how you will process, store and manage this.

In all cases, you will need a basis for processing; a reason for why you are doing something with someone's data. While many organisations have chosen to seek explicit consent, there are grounds for the use of the final principle; Legitimate Interest.

Legitimate interest

There is a clear procedure for deciding what data processing you can cover under legitimate interests. It is not enough to just decide you are going to use legitimate interests, you will need to carefully consider if it is the appropriate data-processing basis for you.

This is a three-part test. You will need to identify a legitimate interest; showing that the processing is necessary to achieve it, and balance it against the individual's interests, rights and freedoms. The ICO breaks it down into the three stages:

1. **Purpose test:** are you pursuing a legitimate interest?
2. **Necessity test:** is the processing necessary for that purpose?
3. **Balancing test:** do the individuals interests override the legitimate interests?

It needs to be applied for each type of data processing you do. Here is an example of a legitimate interest assessment. (please scroll down to page 6)

Consent

The concept of consent in GDPR is stricter than in the previous Act, setting out more onerous requirements in relation to both the content of consent and the way in which it should be obtained. You need to obtain explicit consent to process someone's data, and be clear when doing so, how you will use their data and in what format you will contact them.

Personal Email Communication Regulation (PECR)

GDPR does not replace the existing PECR, which governs the ways in which you can communicate via email. For more information about PECR please click here.

Accountability and compliance

Companies covered by the GDPR will be more accountable for their handling of people's personal information. This can include having data protection policies, data protection impacts assessments and having relevant documents on how data is processed.

Much has been reported about the fines proposed by the ICO for breaches of data – these can be up to €20m. Until the law is in effect it is difficult to know how and when these fines may be applied, so a risk adverse approach in year one is recommended.

Under GDPR, the destruction, loss, alteration, unauthorised disclosure of, or access to people's data has to be reported to a country's data protection regulator – in the case of the UK, this is ICO.

This document explains Accountability and Governance and provides a checklist for when you are preparing for GDPR in your business.

What data does EFFS hold about you and how do we use it?

Participant data in edfringeware

User – To create a user account within edfringeware you must supply certain mandatory personal information.

- Name
- Job Title
- Address (including country and postcode)
- Email
- Telephone number

The only elements of this information accessible to other system users (through a search function) are your name and job title. If you would prefer that other users can't search for you in this way you can opt out via a check box on your user profile page.

Adding a contact – At several points in the system you will be asked to add a contact. These are similar to a user except their information is entered manually into one of the contact fields and they

themselves do not automatically have a user account. These are considered third party contacts. When you create your user account you will have to sign an agreement that you have the permission of that third party to use their information for the purposes of contacts. Depending on the contact this may require fewer mandatory fields be entered.

List of contacts and their purpose

Organisation

- **Organisation Primary Contact** – This is the contact through which most of the Fringe Society's correspondence will take place, including show payout info, signature of any Data Licence Agreement and any edits to your organisation.
- **Organisation Bank Details** – If your show/shows will require a monetary payout at the end of the Fringe due to ticket sales, then you are required to enter the bank details at the organisation level. This includes name of payee, account and sort code and in the case of international banks potentially IBAN or Swift codes. This information is only accessible by administrators of your organisation. Within the Fringe it is only accessible to finance staff and super administrators of the system. This information will never be used for any purpose other than previously stated and will never be shared.
- **Organisation email** – Used primarily as email contact for issues with shows during programme and to provide proofs to.
- **Organisation People tab** –These are people involved with your organisation, to be added here the contact must be, or must become a user in edfringeware.

Venue

- **Type of information** – If entering third party information then all the below contacts require name, email and telephone number.
- **Venue Manager** – Most frequently used as the main venue contact for correspondence with the Fringe Society, and venue manager updates via email
- **Venue Secondary Contact** – Often used as a back-up contact by the venue for correspondence with the Fringe Society and venue manager updates via email
- **Venue Owner** - Rarely used by the Fringe Society except in extreme cases of emergency
- **Venue Media and Marketing Contact** – Often contacted by the Fringe Society Media team in relation to press enquiries
- **Venue Box Office Contact** – Often used by the Fringe Society box office as main contact for all box office correspondence
- **Venue Access Contact** – Often same as box office contact, used by the Fringe Society box office for access related enquiries and bookings service
- **Venue People tab** – These are people involved with your venue, to be added here the contact must be, or must become a user in edfringeware.

Show

- **Type of information** – If entering third party information then all the below contacts require name, email and telephone number. The exception is Show Primary Contact that requires name, address (including country and postcode), email and telephone number.
- **Show Primary Contact** – Most frequently used as main show contact for correspondence with Fringe Society staff, box office, and recipient of bulletins
- **Show Secondary Contact** – Often used as a back-up contact by the venue for correspondence with Fringe Society staff, box office, and recipient of bulletins
- **Show Media Contact** – Often contacted by the Fringe Society Media team in relation to press enquiries, contact will be given out to accredited journalists

- **Show Secondary Media Contact** – Often used as a back-up contact by the Fringe Society Media team in relation to press enquiries, contact will be given out to accredited journalists
- **Show Touring and Development Contact** –Often used by the Fringe Society to contact about development opportunities and shared with professionals who accredit with Arts Industry office
- **Show People tab** – These are people involved with your show, who may or may not be registered in edfringeware.

Show company list

- **Type of information** – Only third party information can be added here. You are required to enter name and job title/role. However, if you wish to request a Welcome Letter for someone on this list then you will also need to provide their date of birth, nationality, passport number/id card number and the city they're travelling to Edinburgh from. If a Welcome Letter is requested (whether needed or not), this information is almost always used by the Fringe Society and if entered will be stored on edfringeware. The Welcome Letter allows non-UK citizens to enter the country, and if provided this will also be stored on FS hard drives in Word and PDF format.

Audience opt-in explained

When a user first signs up to an edfringe.com account using either the website or the app, they're asked to respond yes or no to three optional questions:
- Would you like to sign up to be emailed by the Fringe Society about our products and services? (optional)
- Would you like to sign up to be emailed by the companies of shows that you've purchased tickets for? (optional)
- Would you like to sign up to be emailed by the venues of shows that you've purchased tickets for? (optional)

At the point at which a user purchases tickets, these preferences are sent to VIA (the box office system) and stored against a user's VIA account.

As part of GDPR users must be able to specify the method through which they agreed to be contacted for marketing purposes. You'll notice the statements above only mention email and therefore users can only be contacted using email when permission is granted.

How will we share audience data with you?
Audiences who have opted in to communication from a company or venue have given their consent for the Fringe Society to share their personal data with you. Prior to the Fringe Society transferring any data to you, you must agree to the Data Licence Agreement, which outlines the agreed usage of the data and your liability going forward.

In all cases, data will only be shared once, and with a single named point of contact. No data will be supplied to any further third parties (such as PRs, promotors etc) as there is no legal basis of consent for the supply of this data.

If you are a venue:

The registered Organisation Primary Contact in edfringeware will agree to the Data Licence Agreement. Upon agreement, the Primary Contact may identify a nominated contact to receive the data (such as a Marketing Manager). All data will be transferred to this named contact securely. An Organisation Primary Contact can agree data licencing for all venues within the Organisation group.

If you are a company:

The registered Show Primary Contact in edfringeware will agree to the Data Licence Agreement. Upon agreement, the Primary Contact may identify a nominated contact to receive the data (such as a Marketing Manager). All data will be transferred to this named contact securely. If your company has more than one show, the data licence agreement must list each show.

When can we have the data?

In line with the current legislation, no prior year data will be available after 25 May 2018 unless a customer has given their explicit consent and opted in. Prior year customers were contacted before 25 May 2018 to encourage them to opt in.

In order to manage data processing, storage and retention, data for each Fringe season must be requested by the launch of the Fringe programme in the following year (June). Data requests should be sent to datarequest@edfringe.com.

Data Licence Agreement

"We _____[org/company name]_____ confirm acceptance of the following terms and conditions related data received on behalf of _____[venue/show name(s)]_____ on __/__/20__

Terms and conditions:

Customers should be added to your mailing list, and any correspondence must be related to the services for which they have given consent. For the avoidance of doubt, this means data can only be used in connection with your Edinburgh Festival Fringe activities, irrespective of any year-round activity.

Once data is transferred to your mailing list software (or appropriate alternative) you must delete the supplied data file. This includes email, file storage, network, cloud and other storage types, including removal from your recycle bin (or similar).

The data must not be forwarded or sold on to other organisations, including those with whom you have a working relationship, such as marketing and PR services.

Any time these customers are contacted, they must be given the option to unsubscribe from the mailing list in a clear and easy way.

If a customer opts out of receiving communication directly with your organisation, you must remove them permanently from all lists and not contact them again even if we resupply their details because they have not changed their preferences at the Fringe Society. It is recommended a reliable mailing list service is used to help manage these preferences.

Customer data should be protected always; this includes password protected files, secure, password protected access to mailing list services and ensuring no emails are visible to others when correspondence is sent (ensure emails are BCC'd).

You should have in place a clear policy and process for the removal of customer data, should a customer request it.

Signature to this agreement is confirmation that you accept full responsibility for any data supplied to you and your organisation. As such, any complaint to the ICO that is found to be a result of non-adherence to this agreement will be your liability in all circumstances.

Tips and guidance
Mailing list software – free to use

There are a number of mailing platform options available offering a wide range of scalable features suitable to different budgets.

One of the most popular platforms is Mailchimp which offers a free pricing plan for up to 2,000 subscribers and 12000 emails per month.

A key benefit of using a platform such as Mailchimp is that many of the features that you should be offering as part of GDPR are already there, ready for you to use in the form of pre-built templates and sign up forms.

No matter which platform you decide to use you should always:
- Include the option to opt-out in all emails
- Make it clear to recipients why they are receiving this email (i.e. you are receiving this email as you purchased tickets for XX show during the Edinburgh Festival Fringe, and consent to be contacted by companies and/or venues during the sign-up process)
- Remove inactive contacts from your subscriber list so you're not holding personal information longer than required – there is no point in sending emails to people who aren't opening them.
- Offer your subscribers the chance to give you more information about what they'd like to hear about. This can be done by creating audience groups which can be specified in user preferences.
- Create audience segments and make use of groups to send users information that is of genuine interest to them - you'll receive better results over a blanket approach.

Further reading

ICO guide to GDPR

Full GDPR articles

 Review article on free to use mailing software

Arts guide to GDPR