

# Our guide to the General Data Protection Regulation (GDPR)







# Introduction

The likelihood is if you are currently reading this playbook, you have drawn the short straw and been assigned to “take care of GDPR” for your organisation!

The good news for you is that GDPR should not be seen as something “we have to do”, it should be seen as something we want to do as responsible organisations. The process towards becoming a fully GDPR compliant organisation is about putting our staff and patrons at the centre of what we do.


Here comes the shocking bit: much of what is in the GDPR is already in place under current Data Protection legislation. We should already be fully compliant and only need to make a few changes to fall in line with new additions, but let’s be honest, this is probably not the case.

We’ve developed this playbook in partnership with Eric Hennelly Flanagan, of Riverbank Arts Centre, as an overview of the General Data Protection Regulation (GDPR) and a rough guide on the areas you may need to look at within your organisation. This is not a complete A-Z guide, instead it has been developed to give pointers and prompts, and act as a point of reference to help you on your journey to compliance.

In preparing this guide we would, of course, like to point out that the content of it has been prepared and is provided for general information purposes only. It is not intended to constitute professional legal advice. Although great care has been taken in its preparation, all persons using this guide are advised to seek specific legal advice in relation to any decision or course of action that they wish to take. The responsibility to become familiar with the Regulation and comply with its provisions from 25th May 2018 onwards lies with each organisation individually.

Whilst the GDPR is EU-wide, there may be variances when transposed into law in different member states. As Ticketsolve has customers in a number of jurisdictions, for the purposes of this guide we reference both UK and Irish legislation. We also make references to both the Irish Data Protection Commissioner (DPC) for Irish organisations or Information Commissioner’s Office (ICO) for UK organisations.

We have broken the guide into key areas to help you navigate the legal jargon surrounding GDPR.



This document has been designed to help you and your Organisation understand the new GDPR regulation and the steps you can take to be compliant. It's not designed to offer legal advice and therefore we strongly recommend you seek professional legal advice about your proposed direction before implementing any processes. As the data controller, it's important that you put these processes in place with GDPR compliance in mind and as the data processor, Ticketsolve will provide you with the tools to help with that compliance. We hope this document will help you achieve this.

# What is GDPR?

The EU's General Data Protection Regulation (GDPR) will be brought into EU law on the 25th May 2018. It has been a long time coming, 4 years in fact, and it's all been done to bring data protection of consumers up to scratch for the 21st century.

There has been legislation governing data protection in Ireland since 1988 (Data Protection Act 1988). It was amended by the Data Protection (Amendment) Act 2003.

In the UK The Data Protection Act 1998, supersedes the Data Protection Act 1984 and Access to Personal Files Act 1987. It was amended in 2003. For both jurisdictions, The British-Irish Agreement Act, 1999, Section 51, dealt with data protection in cross border bodies.

The introduction of General Data Protection Regulation will harmonise legislation, not only between Ireland and the UK, but across all EU member states. So instead of having 28 different pieces of legislation we'll have one single law to protect EU citizens. In the case of the UK, regardless of the outcome of Brexit, GDPR will be fully absorbed into UK law.

In tandem with the adoption of GDPR in May 2018, it is envisaged EU members will also be transposing The Privacy and Electronic Communications Regulations (PECR) into law. These regulations govern how you communicate with your customers using electronic means, such as email, text messages and cookies etc. Full details have not been finalised at the time of going to print.

## How will it affect organisations?

GDPR is all about putting your customers in the driving seat when it comes to the data that you hold on them. All organisations that handle the data of EU citizens, irrespective of where the organisation is located, will have to comply with these new regulations. Non-compliance with these new laws may result in significant sanctions, including fines of up to 4% of annual global revenue.

## How will it affect customers?

As we have mentioned previously, GDPR puts the rights of EU citizens first when it comes to their data.

We are lucky because most, if not all, Ticketsolve customers are already extremely careful with customer data. The implementation of GDPR, therefore, should not involve huge changes for most.

For other organisations in different industries this might not be the case, so GDPR aims to give customers protection against these types of organisations.

**GDPR bestows a number of rights to EU citizens that can be summarised as follows:**

- ◆ 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 subject to automated decision-making including profiling

**The right to data portability applies:**

- ◆ to personal data an individual has provided to a controller
- ◆ where the processing is based on the individual's consent or for the performance of a contract
- ◆ when processing is carried out by automated means

Ticketsolve has worked hard on putting much of this in place, therefore changes you will need to make should be minimal.



# What is Personal Data?

When we think of personal data we think of things like name, date of birth, address, contact details etc.

Under EU law, personal data means any information relating to an identified or identifiable natural person.

An identifiable natural person is one who can be identified either directly or indirectly.

## Personal Data

- ◆ Individuals' contact details
- ◆ Educational background
- ◆ Financial and payment details
- ◆ Details of certificates and diplomas education and skills, nationality, job title, and CV
- ◆ IP address

## Personal Sensitive Data

- ◆ Data relating to racial or ethnic origin
- ◆ Political opinions
- ◆ Religious or philosophical beliefs
- ◆ Trade-union membership
- ◆ An individual's gene sequence
- ◆ Fingerprints
- ◆ Facial recognition

# Lawful Basis for Data Processing

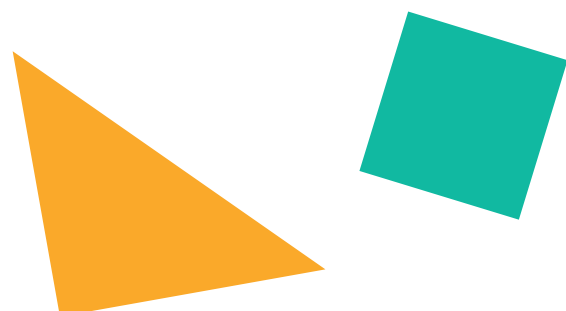
There are a number of legal bases in which organisations can hold and process data. You should look at the various types of data you hold and process, identify your legal basis for having it, and document it. This is particularly important where consent is relied upon as the sole legal basis for processing data. Under the GDPR, individuals will have a stronger right to have their data deleted where customer consent is the only justification for processing. You will have to explain your legal basis for processing personal data in your privacy notice and when you answer a subject access request.

For government departments and agencies, there has been a significant reduction in the number of legal bases they may rely on when processing data. Instead, there will be a general necessity to have specific legislative provisions underpinning one or more of the methods organisations use to process data.

All organisations need to carefully consider how much personal data they gather, and why. If any categories can be discontinued, do so. For the data that remains, consider whether it needs to be kept in its raw format, and how quickly you can begin the process of anonymisation and pseudonymisation.

We have listed below the types of legal basis that we think are relevant to arts organisations. There are more, however we feel that the below will cover all the bases for you. If you would like to see all of the other legal basis please visit the ICO or DPC websites.

- ◆ **Consent** - the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- ◆ **Legitimate Interest** - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject
- ◆ **Performance of Contract** - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract



So, we have the different legal basis for you to process data from your customers but which ones can you use for the different types of data processing? We have covered a few examples below:

## Performance of Contract

You can use this as a legal basis in order to contact your customers about the event they are attending. If the event has been cancelled, you need to send them a pre-event email telling the customer about how to get to the venue or if you want to collect feedback from them following the event, all this is covered under the performance of contract.

## Legitimate Interest

If you decided to use legitimate interest it is important that you are careful and responsible when it comes to sending information to your customers. You must provide evidence as to why you are using this basis for processing your customers data.

Legitimate Interest can only be relied on, where the activity is necessary, and where other legal basis don't exist. Organisations need to balance their needs and the rights and freedoms of the data subject. A full Legitimate Interest Assessment (LIA) should be undertaken.

We have provided you with a template that you can use to write your Legitimate Interest Assessment.

## Consent

Where as legitimate interest is a grey area and you must put forward a case to use it, consent is the opposite, it's black or white. If a customer wants to hear from you, they will tick the box, if not they will leave it unticked. Consent must be explicit, i.e. boxes must not be pre-ticked.

While gaining consent adds an extra layer if you are not already doing so, organisations should see the positives to it, as patrons are saying they actively want to engage with your organisation.

Data processing activities would use consent include marketing emails (covered also by PECR in UK), 3rd party, and other activities that sit outside of performance of contract, and fundraising.

## What is PECR?

PECR is short for **Privacy and Electronic Communications Regulations** and sits alongside the current Data Protection Act in the UK and soon to be GDPR. It is derived from the EU ePrivacy directive 2002/58/EC. The equivalent law in Ireland is Statutory Instrument No. 336 of 2011 which is due to be updated when GDPR becomes law.

PECR gives customers specific privacy rights in relation to electronic communications such as the following:

- ◆ marketing calls, emails, texts and faxes;
- ◆ cookies (and similar technologies);
- ◆ keeping communications services secure; and
- ◆ customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Whilst GDPR will be fully adopted by all member states on May 25th, it is not clear what changes will be made by other member states in relation to EU ePrivacy directive.

# What do you need to do to be GDPR compliant?

The first thing to say about becoming GDPR compliant is that it is an organisation wide concern and all departments need to play an active part in the journey. There is little or no point in a Marketing Manager or Box Office Manager taking on the task, only to have other departments continuing with bad practices.

Part-time/Casual staff are equally as important in ensuring your organisation is compliant.

Think about the entire staff and the points of access they have to data, even minimal, and suddenly you see how many areas of potential breaches you may have.

The second thing you need to remember is to document everything. All meetings, work undertaken etc. relating to GDPR need to be noted. Should issues arise down the line, it's best to have a good paper trail of all the steps the organisation has taken to be compliant.

**Hopefully at this point you have a better understanding of citizens rights and your responsibility to protect them. We've developed a rough checklist of what you should do within your organisation in order to become compliant.**

## 1. Carry out Data Processing Audit

The data processing audit is a vital part of the process. By completing the audit you will show the ICO/DPC that you have thoroughly thought about each data processing activity that your organisation undertakes. It will also get you thinking about what legal basis you have for processing each data set. We have provided you with a handy little template that you can use to enable you to complete this section. We have also given you a few examples of how the template should be completed.

### The main data processing activities that you may undertake:

- ◆ Any communication that is to do with an event use the Performance of Contract legal basis
- ◆ For brochures and mailings to your customers you may potentially use the Legitimate Interest approach but make sure you complete your assessment to show that this legal basis is the correct one for your organisation. Best practice would be to get full consent.
- ◆ Email communication should be done under Consent with clear opt-ins in place.
- ◆ Sharing information with 3rd Party organisations must be done using the Consent basis and each 3rd party organisation must be clearly identified.
- ◆ To contact your customers about your fundraising activities you must ensure that those customers have given their Consent for you to do so.

## 2. Update your Privacy Policy

01. Identify the data controller and Data Processor(s) and provide the name and contact details of the Data Protection Officer or nominated person within the data controller
02. How do you collect personal data (e.g. on-line, face to face, over the phone)?
03. Explain what personal data you are collecting? (for example postal address, email, phone, interests, etc.)
04. Purpose? Outline what you intend using the data for. For example, is it to provide a service to individuals, to send marketing communications to them (where they have agreed for you to do so) and/or for administrative purposes, etc.
05. Detail the individuals' rights where relevant (i.e. to withdraw consent, to object to processing, to request rectification/erasure, submit a Subject Access Request).
06. Explain that people have the right to lodge a complaint with a supervisory authority.
07. What legal basis are you relying on to process the personal data? (e.g. consent, contract, legal obligation, public interest, vital interests or legitimate interests)
08. If you are relying on legitimate interests explain what they are
09. Provide assurances that appropriate safeguards are in place to ensure personal data is kept secure.
10. Consider whether any data is stored or handled outside of the EEA (European Economic Area). If it is state where and what safeguards are in place to keep it secure. Ticketsolve only has EU based servers but you may need to check other third parties.
11. Consider whether you are collecting special categories of personal data and/or children's data. If so explain what extra measures you have in place to offer assurances that it is securely protected.
12. Is the personal data shared with other organisations? If it is shared provide details of the recipients of the data.
13. Make reference to your organisation's data retention policy?
14. If the provision of data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, ensure this is clearly stated together with any consequences of refusing to supply the data.
15. How recent is your Privacy Policy? In line with theme of transparency it is good practice to mention that your privacy policy will be will regularly updated, if that is true, and to detail when your policy was last updated (i.e. month/year).

**Your Privacy Policy should hold all pertinent information about your data processing activities. It should include all information such as:**

- ◆ The different types of legal basis that you will use to process data including legitimate interest, consent and performance of contract
- ◆ Your Cookie Policy
- ◆ Information about how customers can unsubscribe from receiving information from you
- ◆ What third parties, if any, have access to their data
- ◆ How to contact you with regards to any questions they have about their data

We have provided you with an example of a privacy policy you can use which includes all of the above. Obviously, you will have to tailor the policy to take into account your approach, but it should give you a good starting point.

## 3. Review on a regular basis

Now that you have completed your checklist, it is important that you don't just lock all of these documents in a cupboard somewhere and wait until a customer complains or asks questions. You must keep reviewing your processes on a regular basis to ensure that each of your legal basis for processing data are still relevant. We recommend you review your GDPR policies at least every 6 months, and remember document everything so that you can demonstrate that you are compliant.

# How Does Ticketsolve Help?

## Changes we're making to help you comply

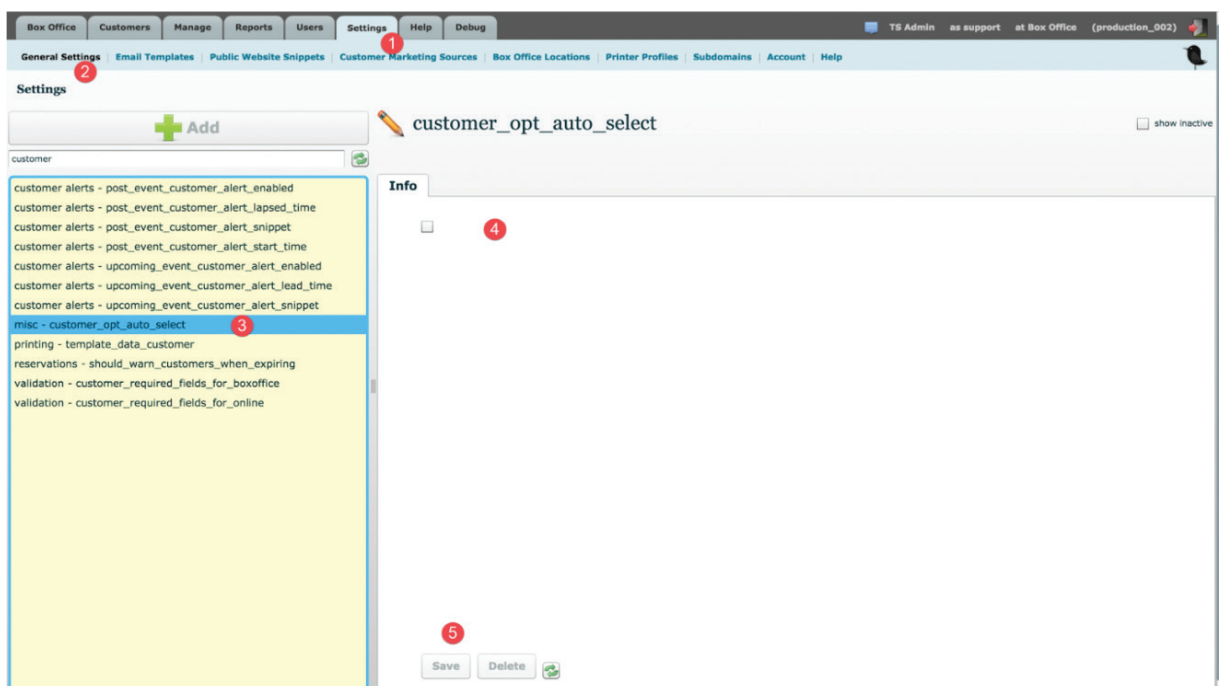
As your ticketing partner we are acutely aware of the need for controls over data. We've been busy behind the scenes over the past 12 months making changes to our system to comply with GDPR ahead of the May deadline. Some of the changes are subtle, others are more apparent. As we continue to develop and enhance the platform, we will add even more features to help with GDPR compliance.

## Changes that you can make within Ticketsolve now!

### Ability to untick opt-in email preference:

Core to GDPR is allowing the customer to 'opt-in' rather than having a marketing preference automatically ticked when a customer gets to that point in the buying process. This is bad practice and you should always have your preferences as opt-in. If you do have your preferences as opt-out, you can change it very easily by:

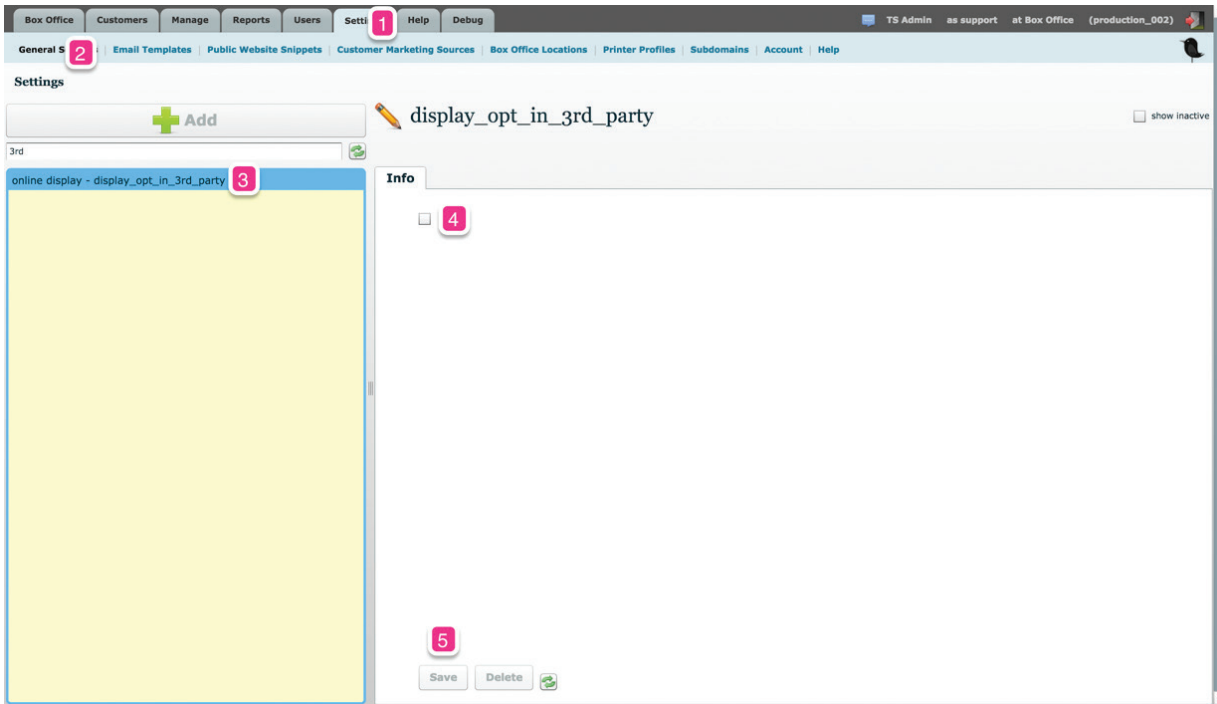
**Going into Ticketsolve, go to 'Settings' > 'General Settings' > 'misc - customer\_opt\_auto\_select' and untick the checkbox, hit save. It's as easy as that.**



## Ability to remove unwanted marketing preferences:

As a system default, Ticketsolve will generally display 4 types of marketing preference options.

To remove an option (as an example we'll use 3rd Party), go to 'Settings' > 'General Settings' > 'online display - display\_opt\_in\_3rd\_party' and untick the tick-box. Hit Save.



## Editing the default system text for all marketing preferences:

Another huge aspect of the new regulation is that all preferences must be granular, unambiguous and easy to understand. Within Ticketsolve you can edit these options by going to:

**'Settings' > 'Public Website Snippets' > and then choose the setting you'd like to change.**

The setting names are;

- ◆ **Email** - 'Public website customer opt-in for email form message'
- ◆ **3rd Party** - 'Public website customer opt-in 3rd party form message'
- ◆ **Mail** - 'Public website customer opt-in for mail form message'
- ◆ **SMS** - 'Public website customer opt-in for SMS form message'

Replace the existing text in the box provided with your desired text and when finished hit save. If you need to include a URL in your text, you can do this by using 'html'.

The screenshot shows the 'Public Website Snippets' management interface. The left sidebar contains a list of snippets, with 'Public website customer opt in for email form message ( 84 )' selected and highlighted in blue. The main area shows the 'Info' section for this snippet, including a language dropdown set to 'English' and a text area containing the default opt-in text. The 'Save' button is visible at the bottom of the text area.

Take a look at a brilliant example below from our friends at the Pavilion Theatre in Dublin. They tell the customer everything they need to know, what they are signing up for, what they will receive and how to unsubscribe.

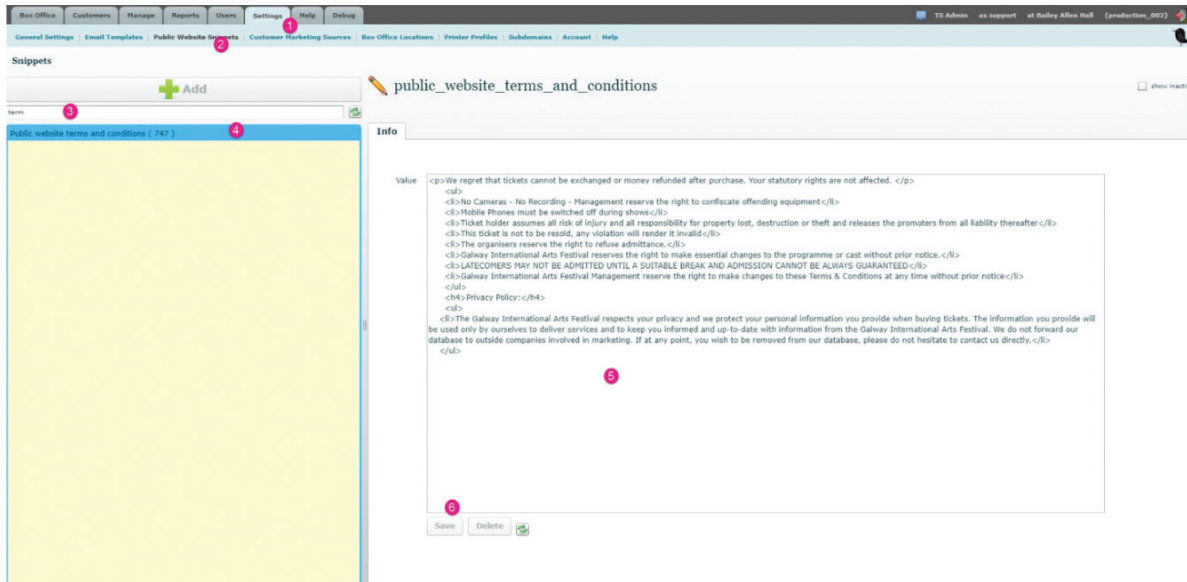
I agree to the [Terms & Conditions](#) (required)

Tick this box to receive updates via E-MAIL. We send one main email every month highlighting our upcoming events and an additional weekly email to our cinema audience highlighting our cinema programme. If at any stage in the future you would like to opt out from receiving these emails, please click unsubscribe at the bottom of any of the emails. (optional)

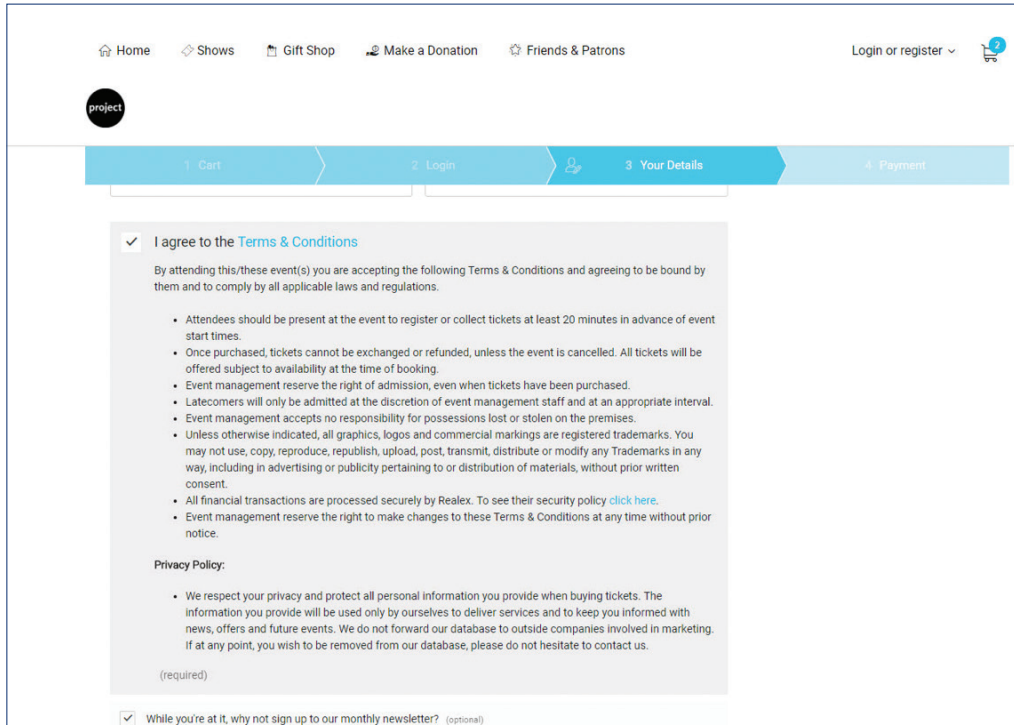
Tick this box to receive updates via MAIL. We post our season brochure to our customers three times a year. Occasionally we post out letters highlighting specific shows and special offers. If at any stage in the future you would like to opt out from receiving post from us, please phone our Box Office 01 231 2929 (optional)

## Editing Terms and Conditions

As GDPR gets closer, you may need to amend your existing Terms and Conditions and perhaps add a link to a Privacy Policy held elsewhere. To find this setting go to the tab **'Settings' > Public Website Snippets > Public website terms and conditions.**



You can add a link to the terms and conditions to show your privacy policy just like Project Arts Centre do below:



## Unlimited opt-ins/Permissions

As part of GDPR, you need to be a little bit more granular with what you ask your customers. For example, it's not good enough anymore just asking them would they like to 'receive emails'. You need to ask, would you like to opt-in for email, then what emails would you like; about events, about fundraising, about arts development and so on (if you go down the consent path).

We are adding in functionality that will allow you to have as many opt-ins as you want, however we will be providing best practice around all this as well. If you ask too many questions, this will interfere with the customer journey and will have an adverse effect on your conversion rates.

### Step 1 - Adding Permission option to your Ticketsolve account

The screenshot shows the 'Permissions' section of the Ticketsolve admin interface. The 'Add' button is highlighted with a red circle '2'. The 'IMMA' permission is selected in the list on the left. The 'Info' tab for 'IMMA' is active, showing the 'Name' field set to 'IMMA' (circled '3'), the 'Active' checkbox checked, and a description: 'Please tick this box if you would like to receive e-mails from IMMA about their events.' (circled '4'). The 'Save' and 'Delete' buttons are at the bottom (circled '5').

### Step 2 - Activating Permission option on your specific show

The screenshot shows the 'Shows' section of the Ticketsolve admin interface. The 'Runs' tab is active, showing a list of shows. 'Yvonne Rainer - Selected Works' is selected. The 'Settings' tab is active, showing a table of settings for the selected show. The 'permission\_options' row is highlighted in blue (circled '4'). Below the table, a list of permissions is shown: '3 - Permission - Test' (unchecked) and '4 - Permission - IMMA' (checked, circled '5'). The 'Save' button is at the bottom (circled '6').

key	account	subdomain	program	show
online_sales_guard_time	60			
onsale_time				
order_qr_codes	false			
permission_options	---	[ ]		
phone_booking_fee_amount	1			
post_event_customer_alert_ema	false			
post_event_customer_alert_sml				
postal_guard_days	5			
preselect_ticket_number	1			
price_description				

### Step 3 - How the new Permission looks to the customer

The screenshot shows a registration form with the following elements:

- Navigation bar: Home, Shows, Vouchers, Make a Donation - Help us Soar!, Friends, Login or register
- Progress bar: 1 Cart, 2 Donations, 3 Login, 4 Your Details, 5 Payment
- Country: Ireland (dropdown), Select Ireland region (dropdown)
- Phone: [input field]
- Email: [input field], Confirm your email address: [input field]
- Agree to the Terms & Conditions (required) [checkbox]
- Check this box to stay on or join the Dublin Dance Festival E-mail list. If you are already on the DDF E-mail list and want to continue receiving e-mails from us, please keep this box checked -- otherwise you will be automatically deleted from the DDF E-mail list, and we'd hate to lose you! (optional) [checkbox]
- Receive updates via mail? (optional) [checkbox]
- Receive updates via sms? (optional) [checkbox]
- Please tick this box if you would like to receive e-mails from IMMA about their events. (optional)** [checkbox] (highlighted with a red box and a pink arrow)
- Any special requirements (e.g. accessibility or other)? (optional) [input field]
- Buttons: Back to previous step, Continue

## MailChimp Integration

As our preferred email marketing platform, we're delighted to see MailChimp make significant changes to help our clients become GDPR compliant.

Some key elements of MailChimp's GDPR offering include:

- ◆ GDPR friendly sign-up forms which provide for a full audit trail.
- ◆ Fully customisable fields for opt-ins (special interests, targeted advertising etc.)
- ◆ Double Opt-In available
- ◆ Easy access to personal data for subject access requests.
- ◆ Opt-Out links are provided with every email sent through MailChimp

The integration of MailChimp with Ticketsolve ensures that Opt-Outs/Out-In are logged and full audit trails exist.

Whilst not a requirement of GDPR, MailChimp allows for double opt-in (customers must click an emailed link to confirm sign up to your mailing list). Best practice would be to implement it as it would provide you with a better defence should a complaint arise for use of data. It also ensures your marketing lists are populated only with customers that actively want to engage.

For your reference here's a piece from MailChimp on their GDPR tools:

<https://blog.MailChimp.com/gdpr-tools-from-MailChimp>

## MailChimp's New Data Processing Addendum

As part of MailChimp's processes, they require you to sign their new data processing addendum. This can be done by going to the web address <https://mailchimp.com/legal/forms/data-processing-agreement/> or you should have had an email on it. It's basically asking you the data controller to agree to MailChimp's new data processing regulations. There is nothing to worry about here, it is part of what is required from MailChimp as part of GDPR, we will be doing the exact same thing in the coming weeks.

One other thing to note about MailChimp is that their servers are based in the US, however as part of this new data processing agreement they have stated that they are a part of the EU-US Privacy Shield, which allows the transfer of data between the EU and US. As part of GDPR, all EU member states have signed off on this new privacy shield meaning using MailChimp is GDPR compliant. For more information on the EU-US Privacy Shield, please visit the link below: <https://www.eci.com/blog/16000-what-you-need-to-know-about-the-eu-us-privacy-shield-and-the-gdpr.html>

# Summary

We hope this guide has provided some help to you on your journey towards full compliance.

For our part, Ticketsolve will continue to provide more help and guidance and updates on developments through our regular emails and blogs. Make sure you are subscribed to our customer mailing list.

We'd suggest following both DPC and ICO across their various social media channels to keep up to date with the changes as they happen. Both offices have fantastic resources on their websites, worth checking out: [www.gdprandyou.ie](http://www.gdprandyou.ie) and [www.ico.co.uk](http://www.ico.co.uk)

**You can, of course, contact our team if you have any questions:**

Phone (Ireland): 01 524 0954

Phone (UK): 01865 987 667

Email: [talktickets@ticketsolve.com](mailto:talktickets@ticketsolve.com)

# Sample Documents

## Legitimate Interests Assessment

### Purpose

Identify the purpose of the processing and the legitimate interests you intend to rely on:

Assessment Question	Response
What are you trying to achieve with the processing?	Awareness. We are processing customer data so that customers who have previously bought tickets with us are aware of any upcoming events that maybe of interest to them.
What is the purpose of the processing?	We can deliver very specific information to previous visitors on shows that are relevant to them.
Who benefits from the processing?	The customer benefits by being informed of specific and relevant events that they have an interest in attending.
Have you identified the relevant legitimate interests?	
What are they?	
Are the noted interests identified as specific legitimate interests under the GDPR or any other legislation?	

# Necessity

Determine if the processing is necessary:

Assessment Question	Response
Can the interests/ objectives be achieved in an less intrusive way?	
Why is the processing necessary to achieve your interests/objectives?	
Is legitimate interests a targeted and proportionate way of achieving your purpose?	

## Balance

Assess your interests against those of the individual and document any safeguarding measures:

Assessment Question	Response
Do you have any relationship with the individual(s)?	
Would people expect you to use their data in this way?	
Does the processing have a minimal privacy impact on the individual(s)?	
How does the processing benefit the individual?	
Can you easily and legibly explain your reasons and interests in a Privacy Notice?	
Are you processing high-risk, special category or confidential information?	
Are you processing children's data?	
Is any individual likely to find the processing intrusive or raise objections?	
Is the processing likely to cause any distress or unwarranted harm?	
Do the rights and freedoms of the individual override your interests?	
Where using legitimate interests for direct marketing, is the individual given the opportunity to opt-out during the initial data collection and via simple, easy to access methods thereafter?	

# Data Processing Audit

## Data Audit

Review all your databases, email lists, spreadsheets, paper documents and other lists of personal data.

Description	
Why is the data held and what is it used for?	
Basis for processing data (e.g. consent, legal, legitimate interest etc)	
Who holds the data and who can access it?	
What security controls are in place?	
What security controls are in place?	
Is this covered by our privacy notice?	
Action Required	

## Data Audit Form Asset Details

Type of Data	
Description of data	
Employee/Department responsible	
Where the data is stored	
Source of the data	
Purpose of the data	
How the data is protected in its storage	
Usage restrictions	
Usage rights	
Usage frequency	
Retention period	
Comments	

# Privacy Policy Example

## Who we are

Company name, how you value your customer data, how you keep the data safe, and what the policy is about.

### Good example from Google:

When you use Google services, you trust us with your information. This Privacy Policy is meant to help you understand what data we collect, why we collect it, and what we do with it. This is important; we hope you will take time to read it carefully.

## Types of data we collect

### Ticketing Data

When you purchase tickets, gift vouchers, merchandise or membership through our Box Office at **X location**, your name, email, phone number, and address data number will be stored by our ticketing partner, **Ticketsolve**.

### Online Data

When you book tickets online, data is shared between **Sample Organisation Realex (payment gateway)**, and **Ticketsolve (ticketing platform)** in order to process the transaction. Where patrons have opted to provide their details for mailings, data will be shared with **MailChimp** (our email partner).

**Ticketsolve** acts as a data processor on behalf of **Sample Organisation** (data controller).

**Ticketsolve**, **Realex**, **MailChimp** and **Sample Organisation** have implemented appropriate technological measures to protect against accidental loss, destruction, damage, alteration or disclosure.

For more information, please see their privacy notices here:

- ◆ MailChimp privacy notice
- ◆ Ticketsolve privacy notice
- ◆ Realex privacy notice

## Website Cookies

When someone visits our website ([www.sample.com](http://www.sample.com)) we use a number of third party services to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site, types of devices used, and length of time on pages.

Cookie	Data	Purpose
Universal Analytics (Google)	_ga _gali _gat_UA-XXXX _gid	These cookies are used to collect information about how visitors use our website. We use the information to compile reports and to help us improve the website. The cookies collect information in an anonymous form, including the number of visitors to the website, device used, where visitors have come to the website from and the pages they visited.

## Disabling cookies

You can prevent the setting of cookies by adjusting the settings on your browser. Be aware that disabling cookies will affect the functionality of this and many other websites that you visit. Disabling cookies may result in the disabling of certain functionality and features of our website.

## Record retention periods

GDPR set's out the principle that personal data shall not be kept for longer than is necessary for the purpose or purposes for which it was obtained.

Sample Organisation has the following data retention periods in place:

Category	Retention Period
<b>Customer Data</b>	
Customer data on Ticketsolve	Removed after X years of inactivity
Customer data on MailChimp	Removed after X years of inactivity
Consent Forms	X years
Photographic Consent Forms	X years
<b>Personnel</b>	
Records of taxes	X years
Records of annual leave, public holiday leave etc.	X years
Recruitment Records (unsuccessful applicants)	X years
Recruitment Records (successful applicants)	X years
Garda Vetting Records	X years
<b>Health and Safety Records</b>	
Accident/Incident Report Forms	X years

## Mailing Lists

When you sign up for our mailing list, either at the time of booking or separately through our sign up form, we collect personal information. We use that information for a couple of reasons: to share information such as upcoming shows; to contact you if we need to obtain or provide additional information; to check our records are right and to check every now and then that you're happy and satisfied. We also gather statistics around email opening and clicks using industry standard technologies to help us monitor and improve our marketing. You can unsubscribe by clicking the unsubscribe link at the bottom of any of our emails or by emailing our data protection officer [DataProtection@Sample.com](mailto:DataProtection@Sample.com).

## Changes to Our Privacy Policy

We may update review and update this policy. This version was adopted on 1/01/1980.

## Access to your personal information

You are entitled to view, amend, or delete the personal information that we hold. Email your request to our data protection officer [DataProtection@Sample.com](mailto:DataProtection@Sample.com).



