

## GDPR Toolkit

### Introduction

This toolkit is designed for organisations/clubs that have created a website on the Pitchero platform. The General Data Protection Regulation 2016/679 ('**GDPR**') is the biggest change to data protection law since the Data Protection Act 1998. It changes your responsibilities in relation to how you collect, hold, use, store and distribute personal data. GDPR comes into force on 25 May 2018 and organisations, such as sports clubs, need to have the relevant policies and procedures in place to ensure that they are compliant with the new legislation. The Information Commissioner's Office ('**ICO**') can issue heavy financial penalties for non-compliance.

This toolkit is designed to highlight some of the steps you should consider taking to achieve GDPR compliance for your organisation's website. This toolkit does not, and is not intended to, constitute exhaustive advice on compliance with GDPR and should be used as a guide only. We strongly recommend that you also seek your own independent legal advice and/or refer to the ICO's guidance on its website for further information. Pitchero will not be held responsible for any GDPR compliance failure that occurs due to your reliance on the information contained in this GDPR Toolkit.

### Privacy Policy

GDPR requires organisations that process (use) personal data to have a privacy policy (also referred to as a privacy notice) in place. A privacy policy provides individuals with information about how an organisation processes personal data.

A privacy policy should be made available to members where you process their data (which includes uploading their personal information to the website). Personal data includes any data relating to an individual who can be identified from that data, directly or indirectly, including but not limited to, an individual's name, identification number, location data, online identifier or one or more factors specific to the physical, health, physiological, genetic, mental, economic, cultural or social identity of that person and in some circumstances, includes photos or recording of individuals.

The checklist below provides you with details of the various information which needs to be included within a privacy policy. The information to be supplied in the policy will differ depending on whether the data is obtained directly from the individual ('**data subject**') or where the data is received from a third party. The checklist should be read in conjunction with the GDPR/GDPR guidance provided by the ICO.

<b>What information must be supplied?</b>	<b>Data obtained directly from the data subject</b>	<b>Data not obtained directly from the data subject</b>
Identity and contact details of the data controller and, where applicable, the data controller's representative/data protection officer	<b>X</b>	<b>X</b>
Purpose of the processing and the legal basis for the processing	<b>X</b>	<b>X</b>
The legitimate interests of the data controller or third party, where applicable	<b>X</b>	<b>X</b>
Categories of personal data to be processed		<b>X</b>
Any recipients or categories of recipients of the personal data	<b>X</b>	<b>X</b>
Details of transfers to countries outside of the EEA and the safeguards in place in these circumstances	<b>X</b>	<b>X</b>

Retention period of data or criteria used to determine the retention period	<b>X</b>	<b>X</b>
The existence of each of the data subject's rights	<b>X</b>	<b>X</b>
The data subject's rights to withdraw consent at any time, where relevant	<b>X</b>	<b>X</b>
The data subject's right to lodge a complaint with a supervisory authority	<b>X</b>	<b>X</b>
The source the personal data originates from and whether it came from publicly accessible sources		<b>X</b>
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	<b>X</b>	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	<b>X</b>	<b>X</b>

Further information regarding privacy policies/notices can be found on the ICO website: <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/>.

### **Data protection policy**

This type of policy is intended for internal use within your organisation. It will be relevant where staff within your organisation process individuals' personal data. This could be in relation to members, guest players, employees, suppliers etc. You should consider including the following information within a data protection policy:

- the name and contact details of the individual responsible for ensuring compliance with data protection legislation and the data protection policy;
- the data protection principles (as set out in the GDPR) and how to comply with them, including;
  - the rights of the individuals whom the data relates to and how to process data in line with these rights;
  - the appropriate security measures that need to be taken against unlawful/authorised processing of personal data and against the accidental loss of, or damage to, personal data;
  - how to deal with data breaches; and
  - when and how personal data can be shared with third parties.

The above is by no means an exhaustive list of what should be included in the policy and it will need to be tailored to reflect how your organisation processes data in practice.

### **Obtaining consent**

Where you collect and upload members or guest players' personal data to the website, in addition to making them aware of your privacy policy, you will also need to obtain the individual's prior written consent. This will be required for example, where you film and upload training sessions or matches or upload photos. The data subject also needs to be informed of their right to withdraw their consent at any time.

If you collect and upload the personal data relating to a child (anyone under the age of 14), you need to obtain the prior written consent of the child's parent or guardian who should also be informed of their right to withdraw their consent at any time.

A practical way of obtaining consent from your members would be to include a consent form (with a link to your online privacy policy) within the pack of registration documents at the beginning of the sporting season. Guest players consent could be obtained by circulating consent forms for signature at the beginning of a match. We have attached some template consent forms links that you can use below. These may need amending to reflect how you process personal data:

<https://s3-eu-west-1.amazonaws.com/files.pitchero.com/gdpr/adult-consent-form.pdf>

<https://s3-eu-west-1.amazonaws.com/files.pitchero.com/gdpr/guest-consent-form.pdf>

<https://s3-eu-west-1.amazonaws.com/files.pitchero.com/gdpr/parental-consent-form.pdf>