


# GDPR GUIDE FOR RMBS, CNAs, Clubs & Leagues



# Contents

INTRODUCTION TO THIS DOCUMENT .....	3
WHAT AM I REQUIRED TO DO?.....	4
1. AWARENESS AND ACCOUNTABILITY.....	6
2. INFORMATION YOU HOLD.....	7
3. COMMUNICATING PRIVACY INFORMATION.....	10
4. INDIVIDUALS' RIGHTS.....	12
5. ACCESS REQUESTS .....	13
6. PROCESSING DATA.....	14
7. CONSENT .....	18
8. CHILDREN .....	19
9. DATA BREACHES .....	20
10. DATA PROTECTION BY DESIGN .....	21
11. DATA PROTECTION OFFICERS.....	23
12. INTERNATIONAL TRANSFERS OF DATA.....	24
LINKS TO MORE INFORMATION AND GUIDANCE.....	25

# Introduction to this document

England Netball have developed this guidance with the aim to help Regional Management Boards, County Netball Associations, Clubs and Leagues (these will collectively be referenced as ‘organisations’) understand the basics of the General Data Protection Regulation (GDPR) and how its requirements will impact you and your organisation. We also hope that it will help you to prioritise and consider what changes may be required. A simple [GDPR Action Plan](#) template has been created for you to monitor compliance. Where you see the following symbol  containing a reference number this indicates it relates to an item on the action plan.

## KEY CHANGES

GDPR does not present a drastic overhaul to the Data Protection Act framework but rather, it plugs gaps, strengthens existing rights and obligations and defines certain concepts more precisely. GDPR will introduce tougher fines for non-compliance and breaches from the Information Commissioners Office (ICO). It will give individuals more say on how organisations use their data, making data protection rules standardised throughout the EU.

For more information about the basic principles of GDPR take a look at these [videos](#)

# What am I required to do?

## KEY DATA PROTECTION PRINCIPLES

There are 6 Data Protection Principles:

**06**

Data is processed in an appropriate manner to maintain integrity and confidentiality

**05**

Retained for only as long as necessary

**04**

Data is accurate and where necessary kept up to date

**03**

Data is adequate, relevant and limited to only what is necessary

**01**

Data is processed lawfully, fairly in a transparent manner

**02**

Data is collected for specified, explicit and legitimate purposes



## WHO IS AFFECTED?

GDPR relates to the protection of “personal data” which is defined as any piece of information that can be used to identify an individual. This could relate to member data, athlete data, event participant data, volunteer data and much more. As a result, the regulation will touch every organisation across the sport sector and will change the way we all collect, retain and use personal information. **GDPR applies to all organisations** whether you pay staff or are all volunteers, whether you have 10 members or 1000 members.

## HOW WILL YOUR ORGANISATION BE AFFECTED?

Your organisation will need to identify someone who will be accountable for your organisation’s compliance (see [Section 11](#)). You need to have a document in place to demonstrate that you have the appropriate controls and risk management in place. The [GDPR Action Plan](#) template will help you achieve this.

The main thing here is to understand what you’re doing with people’s information and why. And to only store minimal data that is required for the purpose it is needed for.

A good place to start is by understanding who is responsible for data you collect:

- **Data Controller** - organisation who manages / collects the data (your organisation, by default).
- **Data Processor** - organisation who uses / handles the data (IT company, any software company you use etc.)

# 1. Awareness & Accountability

Awareness and accountability is all about ensuring the key individuals in your organisation (directors, coaches, volunteers etc.) know that the law has changed. They must understand the importance of GDPR relating to your organisation. For example, they should know that if data from your organisation falls into the wrong hands, you could be fined.

## ACHIEVING AWARENESS AND ACCOUNTABILITY

**1.** Instruct your coaching and administrative staff and volunteers (these will be collectively referred to as 'workforce') to direct any GDPR related requests from your members or their parents directly to you. **1.1** As organisation lead, you will be held responsible for any GDPR related issues.

**2.** Instruct your workforce to record data in the right places. This may be by using your IT software, or any other systems / processes you currently use. **1.2**

**3.** Instruct your workforce on how to communicate with members. Certain communications, (e.g. email conversations about an individual, or where a member is listed by name as attending an event), must be recorded. This can be done using IT software, or other services such as email or spreadsheets. If challenged, you must be able to demonstrate that you have a working system in place. **1.3**

**4.** Ensure Data Protection training is provided to your workforce. **1.4**

**5.** Assess your systems and processes for managing data to ensure they comply with GDPR. **1.5**

**6.** Ensure someone is responsible for regularly reviewing data protection policies and processes. **1.6**

## 2. Information You Hold

Your organisation needs to document the types of personal data you hold, where it comes from and who you share it with.

### TYPES OF DATA YOU HOLD 2.1

This list (though not exhaustive) is a good starting point:

- Name & Address
- Date of birth
- Telephone number(s)
- Next of kin details (may be more than one person)
- Any financial transactions you process
- Any health-related notes / data you keep
- Attendance at your sessions / events
- Which of your groups / teams they belong to
- Any notes / comments you keep about them on file
- Communications where they are mentioned by name
- Any other data you record about them in Word / PDF or using any other documents / programmes



## // 2. Information You Hold

### WHERE INFORMATION COMES FROM 2.2

GDPR requires you to document where the information you hold comes from. In most cases it will be directly from your members or their parents when they join your organisation. But how about non-members?

Do you collect and store information through any other sources, such as Facebook, Twitter, or your website? And how about events / competitions where visitors attend? These need to be thought about and documented, too.

### SPECIAL CATEGORIES OF DATA 2.3

Special categories of data are types of data that are considered more sensitive. For a full list of special category data types visit the [ICO website](#). In the list on the previous page 'health related notes / data' would be considered a special category of data. As well as needing a lawful basis for processing the data you will also need to identify a condition for processing it, such as 'processing is necessary to protect the vital interests of the data subject'. If you process special categories of data you need to document how you process them.





### HOW LONG YOU RETAIN INFORMATION <sup>2.4</sup>

You need to determine an appropriate timescale for retaining data. This could be determined by legal requirements e.g. 7 years for financial information or what seems appropriate e.g. a league retaining the data for the duration of a season or longer if there is justification.

### WHO INFORMATION IS SHARED WITH <sup>2.5</sup>

Sharing information refers to when one organisation 'shares' personal data with another organisation. You must also record who (organisation), if anyone, you share this information with. For example, do you use an IT system to store your members' personal details? Or hold information in email marketing software such as MailChimp? You should already know who has access to your data, so this is one task that will be easy to check off the list.

### USEFUL RESOURCES >>

- Area 2 Template Information Asset Register

# 3. Communicating Privacy Information

## PRIVACY POLICY

Your organisation should have a Privacy Policy (if you already have one it is likely to be found on your website). You need to create a Privacy Policy or update your existing one in line with new GDPR requirements **3.1**. Remember it is important that Privacy Policies are clear and easy to understand. Take a look at England Netball's Privacy Policy for an example.

### THINGS TO INCLUDE

- What information is being collected, how is it collected (e.g. through your website, social media or events) and how is it used (see section 2)
- The lawful processing of information (see section 6)
- Consent and withdrawing consent (see section 7)
- How long you intend to retain the data for (see section 2)
- Children's data (see section 8)
- Who will it be shared with (e.g. IT / email marketing software) (see section 2)
- The individual's rights and how they can exercise these rights (see sections 4 & 5)

Your Privacy Policy should be published. The easiest way to do this is to include it on your website if you have one **3.2**.

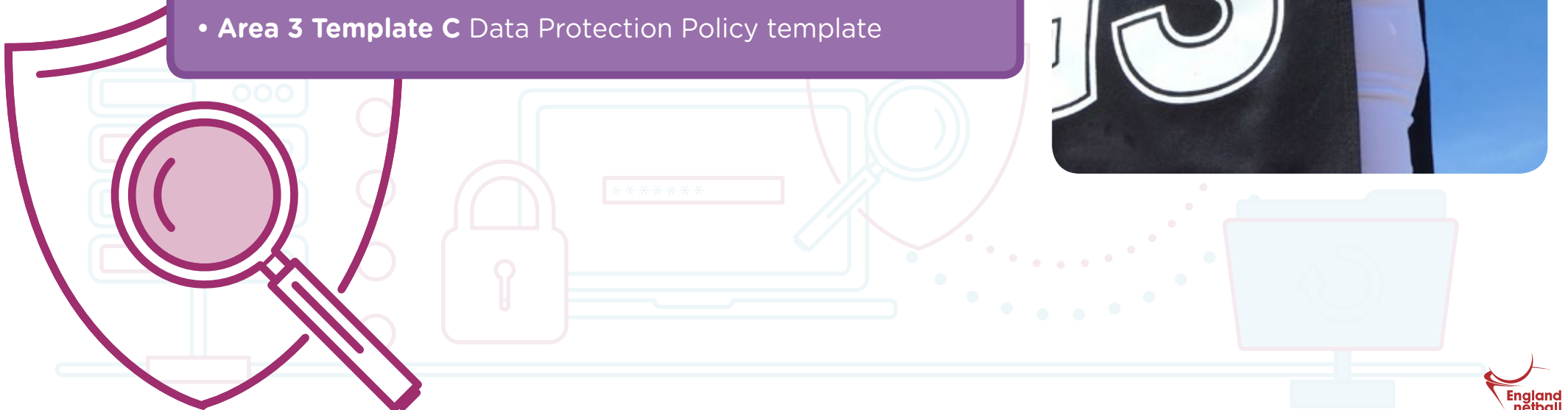
**It is important that Privacy Policies are clear and easy to understand - see our [Guide to Creating a Privacy Policy, Privacy Statements and Data Protection Policy](#) for further information. Alternatively sample Privacy Policies have been produced by the [Sport and Recreation Alliance](#).**

### DATA PROTECTION POLICY 3.3

You should have a Data Protection Policy which details what can and can't be done with the personal data you collect. This should be shared with your workforce. A template Data Protection Policy has been provided.

#### USEFUL RESOURCES >>

- **Area 3 Guide** Creating a Privacy Policy, Privacy Statements and Data Protection Policy
- **Area 3 Template A** Privacy Policy template
- **Area 3 Template B** Privacy Statement template
- **Area 3 Template C** Data Protection Policy template



# 4. Individuals' Rights

GDPR is all about giving individuals enhanced rights when it comes to their data. You should state these rights within your Privacy Policy <sup>4.1</sup>

- 1 Right of access
- 2 Right of rectification
- 3 Right to erasure (right to be forgotten)

***NOTE - a few exceptions may apply here - you mustn't delete records if they are needed:***

- For public health / safety interests, such as safeguarding children.
- To comply with your NGB requirements.
- When making or defending a legal claim.

- 4 Right to restriction of processing
- 5 Right to data portability
- 6 Right to withdraw consent
- 7 Right to object to direct marketing
- 8 Rights in relation to automated decision making and profiling



# 5. Access Requests

## SUBJECT ACCESS REQUESTS (SAR)

You must have a way of dealing with requests by your members for a copy of the information you hold about them **5.1**.

### This includes:

- Any data they've given you about themselves.
- Any information you've recorded about them.
- Information you've collected about them from sources such as Facebook, events and competitions.

### Any handwritten information, as well as digital data you may store, will be required; things like:

- Name & Address
- Date of birth
- Telephone number(s)
- Email address(es)
- Any information about their health

You'll need to provide this information within 30 days in a commonly used electronic format (e.g. Word / PDF / CSV file).

## OTHER ACCESS REQUESTS

In line with each of the data subject rights in section 4, you must find a way to facilitate these rights if they are enacted and document this including timescales **5.2** - **5.4**. Keeping personal information in as few locations as possible will make this a lot easier. You should maintain a log of all access requests you receive and monitor their progress **5.5**.

## USEFUL RESOURCES >>

- **Area 5 Template A** Data Subject Rights Procedures
- **Area 5 Template B** Register of Data Subject Rights Requests and Complaints

# 6. Processing Data

## LAWFUL BASIS FOR PROCESSING DATA

GDPR requires you to document why you need to lawfully process people's data <sup>6.1</sup>. In other words, what information do you keep / use and why?

### For example, things like:

- **Legal** - to fulfil your legal obligations (health and safety, insurance and child protection for example).
- **Contractual** - to allow you to provide members with the services associated with your organisation (such as sending requests for payment, registers, and entrance to events or courses).
- **Benefits** - to send information on things like special offers which have been arranged as part of membership.
- **Marketing** - to send marketing information about partners

**There are 6 lawful bases for processing data. You must decide which of the following are applicable to you and document them within your Privacy Policy:**

### a) **Contract**

You can rely on this lawful basis if you need to process someone's personal data:

- to fulfil your contractual obligations to them; or
- because they have asked you to do something before entering into a contract (e.g. provide information).

## // 6. Processing Data

### b) Legal Obligation

You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation. This does not apply to contractual obligations. You should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation.

### c) Vital Interests

You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life. You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

### d) Public Task

You can rely on this lawful basis if you need to process personal data:

- 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or
- to perform a specific task in the public interest that is set out in law.

It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.

### e) Legitimate Interests

Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate. It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.

The legitimate interests can be your own interests or the interests of third parties.

They can include commercial interests, individual interests or broader societal benefits. You must include details of your legitimate interests in your Privacy Policy.

## // 6. Processing Data

## f) Consent

GDPR sets a high standard for consent. But you often won't need consent this should be the last basis you use when none of the above are applicable. If consent is difficult, look for a different lawful basis. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation. Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.

We believe that for most sports organisations, legitimate interest, contract, consent and legal obligation are relevant. However, you need to decide if these are right for you and your choice(s) need to be documented in your Privacy Policy **6.2**. Take your time to get this right as you must stick by your decision - getting it wrong means breaching GDPR. As part of this process you need to consider how you are going to treat any historic data you hold **6.3**.

**Note:** Organisations with more than 250 employees or which process data classed as sensitive are required to maintain a Register of Lawful Basis and Data Processing Actives (Article 30). Visit the [ICO website](#).





## SYSTEMS & PROCESSES

A system review of all IT and physical systems your organisations use must be conducted [6.4](#). As part of this you should consider the following:

- If your organisation has assets (e.g. laptops, phones etc.) is your asset register up to date [6.5](#)
- Do you have the appropriate security measure in place for processing any special categories of data [6.6](#)
- Is any data being processed outside of the EEA and if so do you have the necessary protections in place? [6.7](#)
- Document how you will ensure personal data is up to date [6.8](#)
- Are your IT systems regularly backed up [6.9](#)
- If you share personal data with 3rd Party processors check they have the appropriate security measures in place and you have a data sharing agreement with them [6.10](#)
- If you act as a 3rd Party processor for another organisation ensure you have a data sharing agreement in place [6.11](#)
- Ensure you have a process for destroying data e.g. IT assets, confidential waste [6.12](#)

## USEFUL RESOURCES >>

- **Area 3 Guide** Creating a Privacy Policy, Privacy Notice and Data Protection Policy
- **Area 3 Template A** Privacy Policy template
- **Area 6 Template IT** Asset Register

# 7. Consent

When using consent as the legal basis for processing data you must be very open about why you process data and what people are consenting to.

## GAINING CONSENT UNDER GDPR

- You cannot rely on inaction when filling in forms - having pre-checked tick boxes would not count as giving consent. You must make sure that people actively 'opt in' (by clicking a tick box for example) to agree to any data processing you undertake which relies on the consent basis for processing.
- You must ask people to agree that you can use their data in each of the ways you outline in Step 6. Update any forms used for collecting data **7.1**.

## WITHDRAWING CONSENT

You must make it easy for people to withdraw their consent at any time and are required to ensure they know how **7.2**. They could do so by:

- Updating a form on your website.
- Logging in to your IT software and changing their preferences.
- Outlining their request in an email to your organisation's Data Protection Lead.

## USEFUL RESOURCES >>

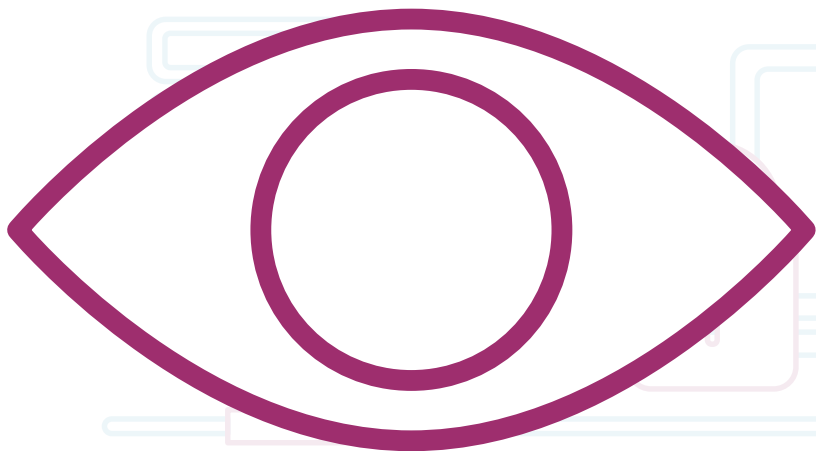
- **Area 3 Guide** Creating a Privacy Policy, Privacy Notice and Data Protection Policy
- **Area 3 Template B** Privacy Notice template

# 8. Children

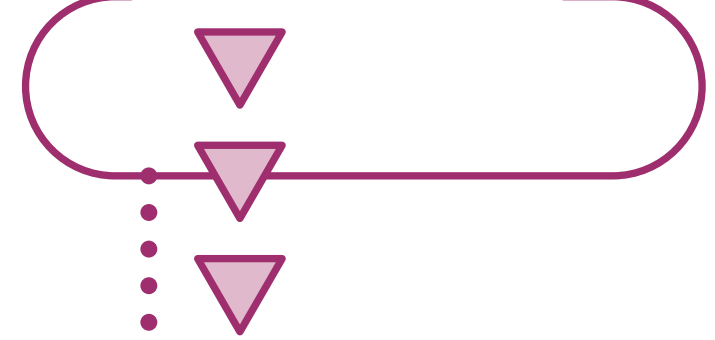
If you don't already, you'll need to get consent from a child's parent or guardian to process their data. Under GDPR a child aged 14 or above will be able to give their own consent. It is recommended to produce a Privacy Policy for Children designed to be easily understandable. Once the ICO have considered feedback on their initial suggestions about children and GDPR, they will produce additional final guidance.

Consent must be gained for each different type of communication you plan to send (such as those outlined under point 7 in this guide) **8.1**.

When sending texts / emails to children, you should really follow the [NSPCC's CPSU](#) best practice guidelines here **8.2**.



# 9. Data Breaches



Under GDPR you will need to develop a way of dealing with potential 'data breaches' 9.1  
Data breaches don't just happen digitally, but also in the physical world.

## Here are some examples:

- Printed folders / files containing peoples' details are lost or stolen.
- Someone gains unauthorised access to your IT software, data or files.
- You (or one of your workforce) lose a mobile phone that has club / member details on it.
- You (or one of your workforce's) computers, with organisation details on it, gets a virus or is hacked.
- Your IT software is hacked.

If you have a breach, you must be able to detect, report and investigate it. We have created a Security Incident / Breach Process Flowchart to help you with this. You may need to report it to the ICO and the members / parents concerned. Remember, failure to report a breach could result in a fine, as well as a fine for the breach itself.

## USEFUL RESOURCES >>

- **Area 9 Guide** Security incident / Breach Flowchart
- **Area 9 Template** Register of Security Incidents / Breaches

# 10. Data Protection By Design

## PRIVACY BY DESIGN

GDPR makes 'privacy by design' an express legal requirement. You need to make sure that the processes you implement are designed with data privacy at the forefront.

As part of this, you may need to complete a Data Protection Impact Assessment (DPIA) which should assist you to highlight any potential problems with the way you handle data **10.1**. DPIAs are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

The GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in a high risk to individuals' interests for example 'sensitive data or data of a highly personal nature'. The ICO also requires you to do a DPIA if you plan to use new technologies. The need for a DPIA can be identified as part of the project management process or by completing screening questions (**Form 1 in the DPIA Tool**).

If you don't need to conduct a DPIA you should document your decision by saving Form 1 from the DPIA Tool **10.1**.



## CONTRACTS

If you enter into any contracts with organisations which will involve data sharing or processing you must ensure that the content of the contracts contains appropriate data protection clauses.

## SECURELY SHARING AND SENDING DATA

Sharing data is when an organisation shares personal data with another organisation and a data sharing agreement should be in place. Sending data is the mechanism of transferring data, this could be both between individuals within your organisation as well as to another organisation.

You must ensure that whenever you 'send' personal data you do so securely. This relates to the secure sending of hard copy data as well as electronic data. You should always make sure electronic data is encrypted e.g. password protected.

### USEFUL RESOURCES >>

- **Area 10 Guide A** Data Protection Impact Assessments (DPIA)
- **Area 10 Template** Data Protection Impact Assessment Procedure
- **Area 10 Guide** How to Encrypt and Send Electronic Data.

# 11. Data Protection Officers

## Under the GDPR, you must appoint a DPO if:

- you are a public authority;
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

Most large organisations or groups of companies must legally have a nominated Data Protection Officer (DPO), whose specific job it is to look after all GDPR related issues. There is no definitive answer that can be applied carte blanche to every organisation but it is likely that most RMBs, CNAs, Clubs and Leagues will not need to appoint a DPO <sup>11.1</sup>. However, it is important that someone within the organisation is delegated as a Data Protection Lead to ensure your organisation is GDPR compliant <sup>11.2</sup> and you should update role descriptions to reflect any additional data protection responsibilities <sup>11.3</sup>.

You can appoint a DPO if you wish, even if you aren't required to, but if you decide to voluntarily appoint a DPO you should be aware that the same requirements of the position and tasks apply had the appointment been mandatory under the GDPR.

# 12. International Transfers Of Data

This will not apply to most sports organisation in the UK.

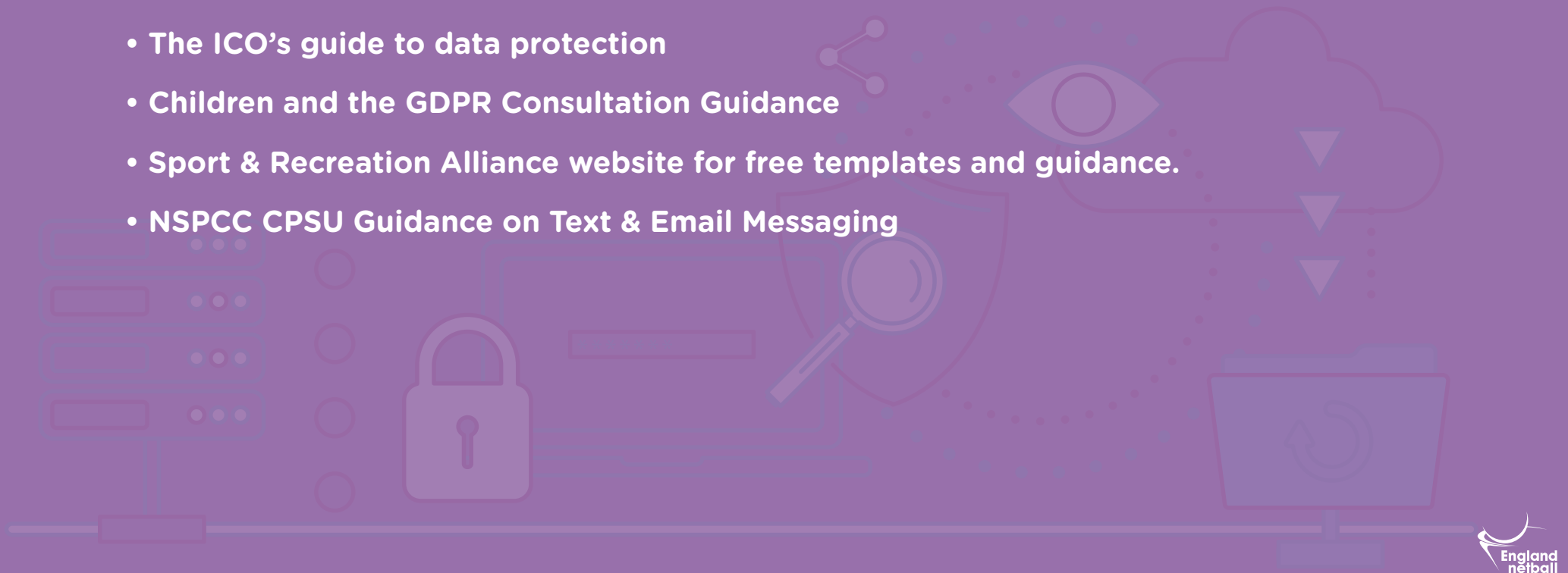
However, if your organisation operates (has offices or a physical presence) in any other EEA member states outside of the UK, you will need to determine and document your lead data protection supervisory authority [12.1](#).





# Links to more information and guidance

- More guidance for communicating privacy information
- Check whether you need to register your club with the ICO (fee may be required)
- Getting ready for GDPR - the ICO checker tool
- The ICO's guide to data protection
- Children and the GDPR Consultation Guidance
- Sport & Recreation Alliance website for free templates and guidance.
- NSPCC CPSU Guidance on Text & Email Messaging



# England netball

