GDPR INFORMATION SEMINAR

Dun Laoghaire / Rathdown Sports Partnership

March 2018

Leman
SOLICITORS

IMPORTANT MESSAGE FROM MANCHESTER UNITED

WHY ?

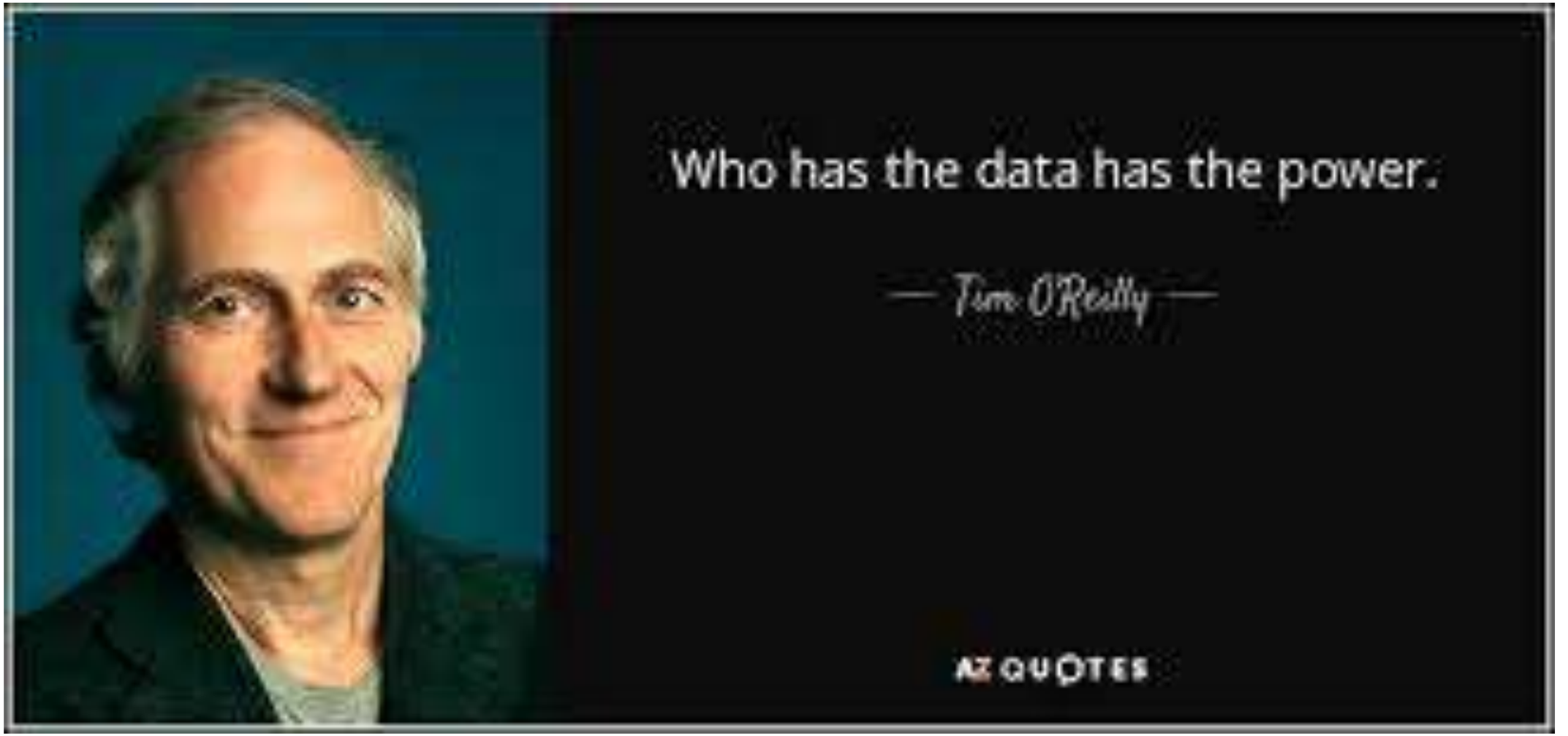
1. GDPR applies to you because you hold data – it does not discriminate on size / profit
2. Deadline to comply
3. Fines
4. Book stops with you ?
5. Piece of mind!

Agenda

1. Why is data so important ?
2. What is GDPR?
3. Fines and deadlines
4. Terminology
5. Principles of Data Protection
6. How does it affect my club?
7. 9 Steps to compliance
8. Key Messages
9. Q&A

Leman
SOLICITORS

Why is data so Important



So who know's what they're talking about ? !

What is GDPR? – General overview

- General Data Protection Regulations (“GDPR”) - New EU Regulations regarding Data Protection
- Replaces existing Irish Law
- Same principles generally apply.
- Purpose of GDPR ?
- Protects your data
- *“Data is power and the New oil” !*

What's new – GDPR – Key Provisions

1. **Extra territorial effect**
2. **Higher Sanctions - up to €20m or 4% of undertaking's global turnover of more**
3. **Consent is defined**
4. **Must notify DPA without delay within 72 hours of breach**
5. **New role of Data Protection Officer**
6. **Controllers and processors jointly liable**
7. **Right to erasure (be forgotten) subject to various conditions**
8. **Right to rectification, if inaccurate**
9. **General right not to 'profiled'**
10. **Privacy by design introduced**
11. **DP Impact assessments must be prepared**
12. **Right to restrict (freeze) processing**

The ‘Lingo’

1. ***Data Subject*** = employees / past employees /prospective employees / members / players / coaches / volunteers / visitors

2. ***Data Controller*** = Employer / club / sports body

3. ***Data Processor*** = HR provider / healthcare provider / sub-contractors / 3rd party administrators

4. ***Personal Data*** - *Data from which a living person can be identified:* Name, address, date of birth, PPS or telephone number, bank details, email address etc…

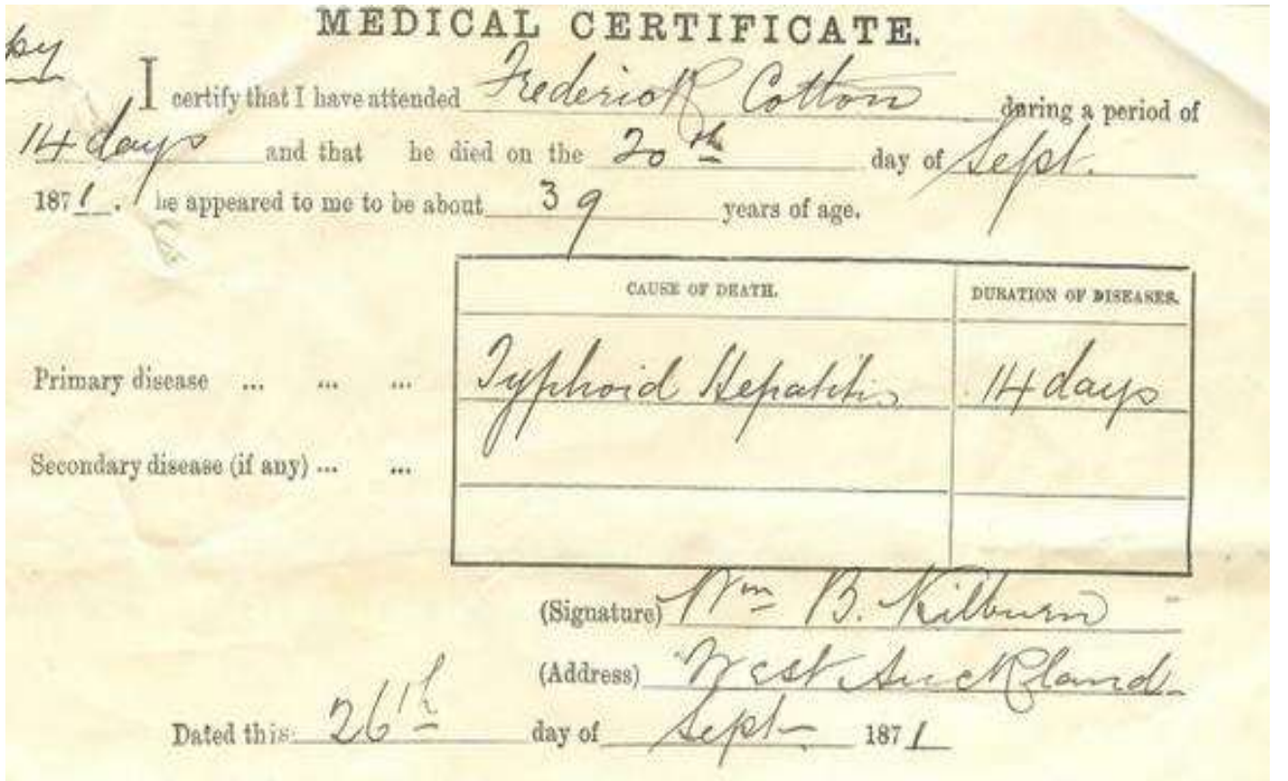
Personal data you hold

- Name
- Date of birth
- Address
- Telephone number(s)
- Next of kin details
- Membership forms
- Any financial transactions you process
- Any health-related notes you keep
- Attendance at your classes / events
- Names of groups / teams
- Any notes / comments you keep about them
- Communications where they are mentioned by name
- Teamsheets
- Photo’s / voice-recordings

- **Anything that identifies a person**

Sensitive Personal Data

1. Trade union membership
2. Racial or ethnic origin
3. Political opinions
4. Religious beliefs
5. Sexuality
6. Commission of an alleged offence
7. Physical or mental health or condition
8. Biometric data (fingerprint etc…)



MEDICAL CERTIFICATE.

I certify that I have attended Frederick Cotton during a period of 14 days and that he died on the 20th day of Sept. 187 1. he appeared to me to be about 39 years of age.

	CAUSE OF DEATH.	DURATION OF DISEASES.
Primary disease	Typhoid Hepatitis	14 days
Secondary disease (if any)		

(Signature) Wm B. Kilburn

(Address) West Auckland

Dated this 26th day of Sept. 187 1

Where is the personal data held ?

- Physical membership application forms (summer camp)
- Online subscription payments
- Teamer / Whatsapp / Social media
- Emails and devices
- File sharing / dropbox
- Ezine contact lists
- Internal spreadsheets
- Garda Vetting info
- Teamsheets, training attendance lists
- Information captured on club websites

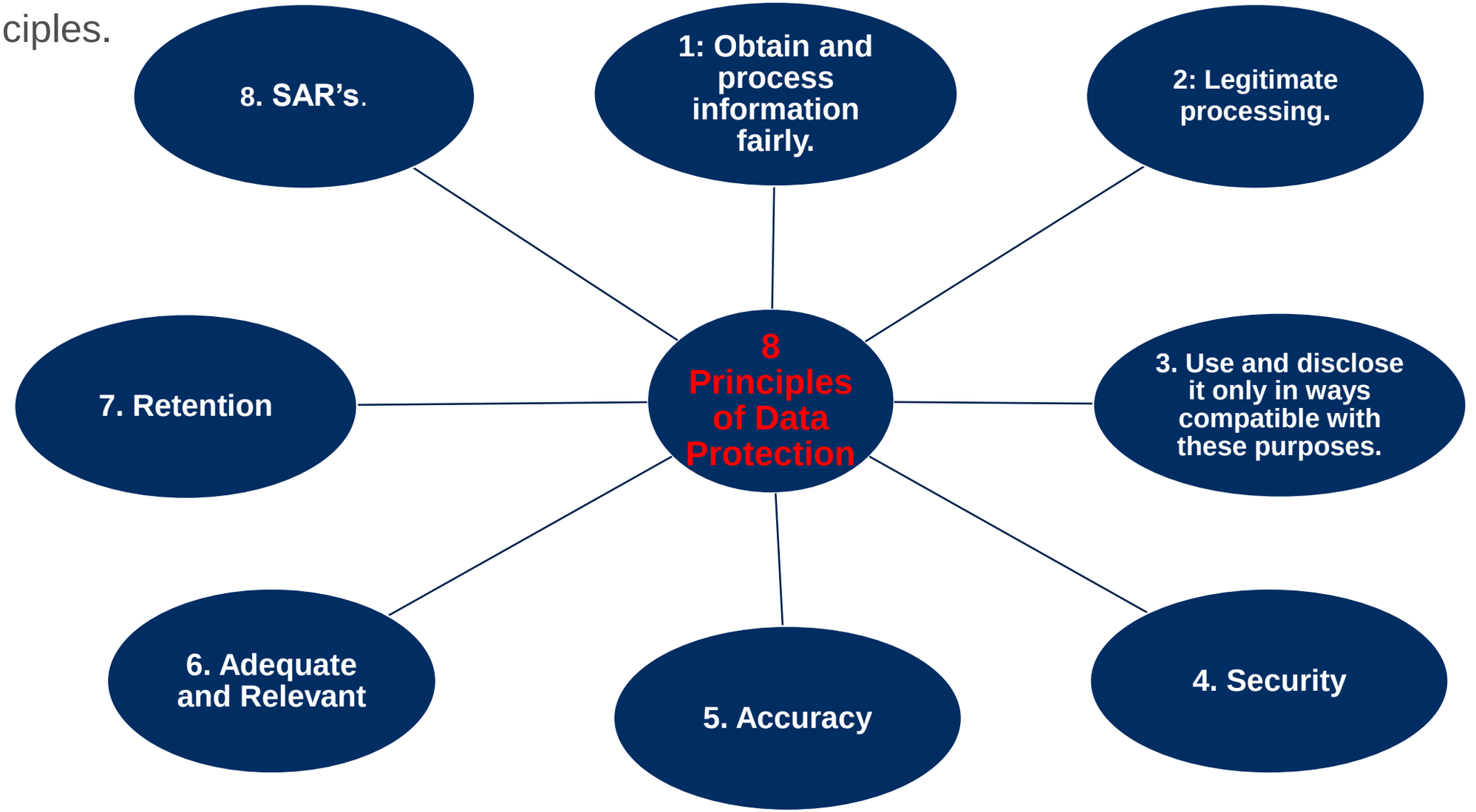
Why are sports clubs subject to GDPR ?

Your club holds personal data in multiple silo's

- You are a **Data Controller** – because you have the personal data of members & volunteers
- You now must decide how and why personal data is processed.
- Must comply with certain GDPR principles

What principles do I need to comply with ?

Same Principles.



How could non-compliance affect your club?

- **Fines**

- **Turnover =** Membership subscriptions, Grants, Bar and restaurant sales, Commercial sponsorship, Fundraising initiatives

- €200,000 turnover = €8,000 per breach

Other Factors:

- Reputational risk
- Criminal sanctions

What is a data breach?

1. Lost folders / files containing peoples' details are lost or stolen.
2. Someone gains unauthorised access to your club software, data or files.
3. Lose a mobile phone / laptop that has club / member details on it.
4. Computers, with club details on it, gets a virus or is hacked.
5. Your club management software is hacked.

What do you do when a Data Breach happens

- **Must notify DPC within 72 hours of breach** leading to accidental or unlawful data destruction, loss, alteration or unauthorised disclosure.

- **Must Notify data subject** unless breach unlikely to result in a risk

Who enforces GDPR in Ireland ?

- ODPC
- Independent body which has responsibility for safeguarding data in Ire.
- Individuals can complain to DPC. Powers to investigate / fine etc…
- See guidance on (www.gdprandyou.ie)

9 Steps to ensure compliance with GDPR Principles

STEP 1

Develop a Data Protection Policy Document

To include an outline of how your club handles personal data…..

….including the following procedures and decisions:

STEP 2

Appointments plus education

1. Educate key officers and volunteers handling data
2. Identify likely problem areas now that could cause GDPR compliance issues
3. Put a project team together
4. Appoint a person responsible for Data Protection in the club and make all members aware of this. A “data protection champion”

STEP 3

Create an Inventory of **ALL personal data you hold and examine:**

1. Why is it being held?
2. How was it obtained?
3. Why was it originally gathered?
4. How long is it being retained for?
5. How secure is it (encryption / passwords and accessibility)?
6. Is it shared with any third parties?

If you don’t need it - stop collecting it

Prioritise sensitive personal data measures

STEP 3 cont….

Processing Data – Why ?

Ask yourself – why am I holding the Data
There are 6 lawful bases for processing data.

You must decide which of the following are applicable to you:

1. consent;
2. contract;
3. legal obligation;
4. vital interests;
5. public task; or
6. legitimate interest.

For most sports clubs, **legitimate interest, contract and consent are sufficient.**

Your choice(s) need to be documented.

Inventory example

#	Processing activity	Purpose	Category of data processed	Categories of data subject	Categories of Recipient	Format	Where Held	Accessible by	Retention Period	3rd party access
	Membership forms	To capture personal info and contact details for members	Personal Details incl. • Name, • DOB • Etc…	Members, Children and Juvenile players	Used internally within the club only	Paper	Club house	Club Exec /Sec	1 Year	None
	Online Membership forms	To capture details of members and to facilitate payment of fees	As above plus **Financial details** incl. BIC & IBAN	As above	Shared with AIB Bank and internally	Electronic	Hosted in Web Services data centre, Athlone,	Authorised users on the system.	1 Yr	Data Processor
	Whatsapp	To notify players on adult teams of training, matches etc..	Name, phone no. etc….	Adult players and coaches	N/A	Electronic	Whatsapp	All members on Whatsapp group	1 yr	Whatsapp

STEP 4

Develop a privacy policy

Your club should have a **privacy policy** in place (likely to be found on your website).

This will need updating in line with new GDPR requirements. Use concise, simple language

Things to include:

1. What information is being collected and by who?
2. How is it collected (eg through your website, social media or events) and how is it used?
3. The lawful processing of information.
4. Who will it be shared with (eg your club management / email marketing software)?
5. What will the effect of this be on the members / parents concerned?
6. Is the intended use of this info likely to cause members / parents to object or complain?

STEP 5

Subject Access Request awareness

GDPR is all about giving individuals enhanced rights when it comes to their data.

These rights include:

- Subject Access Requests (any member can request copy of ALL information held about them)
- To have inaccuracies corrected
- To have information erased
- To object to direct marketing
- To restrict processing of their information including automated decision making

STEP 6

Subject Access Requests Policy

You must have a **policy** of dealing with requests by your members for a copy of the information you hold: This includes:

1. Any data they've given you about themselves.
2. Any information you've recorded about them.
3. 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:

- Name / Date of birth / Address /Telephone number(s) / Email address(es)

Review current procedures:

- How long to locate (and correct or delete) the data from all locations where it is stored?
- Who will make the decisions about deletion?
- Can you Automate your data ?

Provide in 30 days in electronic format (eg PDF file).
Look out for the **Disgruntled Member !**

STEP 7

‘Opt – in’ Communication

- Consent – must be ‘freely given, specific informed and unambiguous
- You must send an ‘opt-in’ communication to your member if you want to legally send them notifications or if you want to use their data for marketing purposes.
- Will be required for marketing
- Requires indication of **positive agreement**
- Consent can be withdrawn
- Must have clear audit trail showing how consent was given
- Other options:
  - Legitimate interest
  - Legal obligation
  - Carrying out contract
- Need to explain in privacy notice

Getting Consent

Make sure that people actively ‘opt in’ (tick box)

This could look like:

1. *I agree for you to use my data for legal reasons associated with the running of your club.*

2. *I agree for you to use my data so that you can provide me with your club’s services.*

3. *I agree for you to use my data so that I can receive the benefits and special offers associated with being a member of your club.*

Withdrawing consent

You must make it easy for people to withdraw their consent at any time and are required to ensure they know how.

They could do so by:

1. *Updating a form on your website.*

2. *Logging in to your club management software and changing their preferences.*

3. *Outlining their request in an email to your club’s Data Controller.*

Step 8

Processing Children’s Data

Does your club work with children ?

Do you have adequate systems in place to verify individual ages and get consent from guardians?

Special protections for children’s data in GDPR particularly in the context of social media and commercial internet services

Consent needs to be verifiable and communicated to your underage members in simple language.

Ireland looks set to adopt 13 as the age at which a child can consent to data processing without specific parental permission

STEP 9

Require DPO ?

Required if **core activities** involve systematic monitoring or large scale processing of sensitive data or a public body

ANSWER – Probably unlikely for your Club

BUT …. Every Club should have a “Data Protection Champion”

And … record reasons for not having DPO in

RECAP - What should your organisation be doing?

- Identify roles and responsibilities before work begins:
  - GDPR Project Team
  - DP Champion

- Set realistic expectations and timelines for the level of effort required to complete the project.

- Areas for consideration:
  - Personal Data Inventory
  - Review Consents
  - Review 3rd party Contracts
  - Data Privacy Policy
  - Email Marketing
  - Staff Training
  - Privacy Notice

Leman
CONSULTING

- Legal Audit
- GDPR
- Digitisation
- Legal Department Analysis & Design
- Legal Technology Advisory
- Data Capture
- Smart Contracts
- Training

Our Services

LEMAN CONSULTING

- Leman Consulting assists NGB's and clubs in delivering immediate compliance with GDPR

- If you don't have expertise or resources to implement before 25 May, then let us know !

Contact Us

Morgan Crowe

Solicitor, Sports Law Team,
Leman Solicitors

mcrowe@leman.ie

Karl Manweiler

Managing Director, Leman Consulting

kmanweiler@leman.ie

Larry Fenelon

Director, Leman Consulting

lfenelon@leman.ie

Questions & Answers