GENERAL DATA PROTECTION REGULATIONS (GDPR)

A SHORT GUIDE FOR CLUBS AND BRANCHES

Hockey Ireland

What is GDPR and how does it affect me?

GDPR - the new EU regulations regarding Data Protection. It comes into effect on 25th May and will implement uniformity across Europe. It replaces existing Irish law.

The purpose of GDPR is to protect data

GDPR applies to you because you hold data – it does not discriminate on size / profit

No matter how big or small your club is, if you collect, handle or keep people's data you need to do it correctly. Any personal details which you ask for from players, coaches, volunteers – in fact anyone associated with your club – must be taken and stored correctly. This is even if it is just their name or an email address.

What's new

Extra territorial effect
Higher sanctions – up to €20m or 4% of turnover
Consent is defined
Must notify DPA within 72 hours of breach
Controllers and processors jointly liable
Right to be forgotten
Right to rectification if data is not accurate
Right not to be 'profiled'
Privacy by design introduced
DP Impact Assessments must be prepared
Right to freeze processing

Principals your club needs to comply with

- Obtain and process information fairly
- Legitimate Processing (Why)
- Use and disclose only in ways compatible with these purposes
- Security – where – who has access
- Accuracy – is the data correct
- Adequate and Relevant
- Retention – how long will it be kept for
- SAR's

How to use personal data

Your club needs to have a rigorous process when it comes to handling data. Data should be:

- Processed securely
- Only what your club needs
- Updated regularly and accurately
- Only shared if the individual has given consent
- Only used for the purpose for which it was collected

Who's Who, What's What

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

2. Data Controller = Club / Branch / Hockey Ireland/ IHUA

3. Data Processor = HR provider / insurance provider / self-employed coaches / membership service providers

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…

Hockey Ireland

Examples of Personal Data that Clubs 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 events
- Names of groups / teams
- Any notes / comments you keep about them
- Communications where they are mentioned by name
- Teamsheets
- Photo's
- **Anything that identifies a person**

DATA SUBJECT MUST GIVE CONSENT

Membership Application Form

Contact Information

Child's Name: _____ Phone: _____

Street Address: _____

City, State, ZIP: _____ Date of Birth: _____

Parent Information

Father's Name: _____

Address (if different) _____

Father's Occupation: _____ Phone: _____

Mother's Name: _____

Address (if different) _____

Mother's Occupation: _____ Phone: _____

Referral Information

Please enter the contact information in the space provided below the person who referred your child to our group/organization.

Name: _____ Phone: _____

Street Address: _____

City, State, ZIP: _____

Emergency Contact Information

Emergency Contact: _____

Relation to Contact: _____

Phone: _____

By signing below, you agree that all information you have provided in this application are true, to the best of your knowledge.

Signature _____ Date: _____

Examples of Sensitive Personal Data

- Trade union membership
- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Sexuality
- Commission of an alleged offence
- Physical or mental health or condition
- Biometric data (fingerprint etc…)

- **DATA SUBJECT MUST GIVE EXPLICIT CONSENT**

Where is the 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

India

#	Name	Min	1st	2nd	3rd	4th
4	MOR Mandeep					
6	KUMAR Surender	X				
8	SINGH Sardar (C)	X				
9	SINGH Gurjant					
10	SINGH Simranjeet	X				
12	TIRKEY Dipsan					
13	KARKERA Suraj (GK)	X				
15	SANNUVANDA Uthappa					
17	SUMIT	X				
18	SHARMA Nilakanta					
19	PATHAK Krishan (GK)					
20	SINGH Talwinder	X				
22	KUMAR Varun	X				
23	XESS Nilam	X				
28	KUMAR Sumit	X				
30	ROHIDAS Amit	X				
31	SINGH Ramandeep	X				
32	LAKRA Shilanand					

Ireland

#	Name	Min	1st	2nd	3rd	4th
2	CARR Jamie (GK)	X				
4	BELL Jonathan (C)	X				
5	BELL Matthew					
7	O'CONNOR Sam					
8	CARGO Chris	X				
10	SOTHERN Alan	X				
12	MAGEE Eugene					
15	SHIMMINS Kirk	X				
16	O'DONOGHUE Shane	X				
17	MURRAY Sean					
18	McKEE John	X				
21	DALE Julian					
22	ROBSON Michael	X				
26	GLEGHORNE Paul	X				
29	COLE Lee	X				
30	LOUGHREY Stuart	X				
31	INGRAM Mark (GK)					
32	COLE Stephen					

What is a Data Breach?

- Lost Folders / files containing peoples details are lost or stolen
- Someone gains unauthorised access to club data
- Lose a mobile phone / laptop with club members details on it
- Computers with club details gets hacked
- Club management software his hacked

What to do if a Data Breach happens

- Must notify DPC with 72 hours of breach leading to accidental or lawful data destruction, loss, alteration or unauthorised disclosure
- Must notify data subject unless breach unlikely to result in a risk

STEPS TO COMPLIANCE

Step 1: Develop a Data Protection Policy Document

Step 2: Appointments plus education:

- Educate key officers and volunteers handling data
- Put a project team together
- Appoint a person responsible for Data Protection in the club and make all members aware of this - a "Data Protection Champion".

Step 3: Do an inventory / audit of ALL personal data you hold and examine:

- Why is it being held?
- How was it obtained?
- Why was it orginally gathered?
- How long is being retained for ?
- How secure is it (encryption / passwords and accessibility)?

If you don't need it – stop collecting it

Prioritise sensitive personal data measures

Step 3 Cont'd:

Processing Data – Why – ask yourself why am I holding the data. There are 6 lawful bases for processing data:

Consent – contract – legal obligation – vital interests – public task or legitimate interest

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

Your choice needs to be documented in Privacy Policy

Inventory / Audit 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 of the system	1 year	Data Processor

Step 4: Develop a Privacy Policy

Your club should have a Privacy Policy in place (likely to be found on your website).

Things to include:

- What information is being collected and by who
- How it is collected and how it is used
- The lawful processing of information
- Who it will be shared with
- What will the effect of this be on the members / parents concerned
- Is the intended use likely to cause members to complain

Step 5: Subject Access Request Awareness

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

- Right to be informed
- Right of ….access
  rectification
  erasure
- Right to ….object
  restrict processing
  data portability
- Rights in relation to automated decision making and profiling

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 can be detailed in Data Protection Policy). This includes:

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

Any handwritten information as well as digital data:

- name/DOB/ address/ phone no / email address

Review current procedures

- How long to locate (and correct or delete) data
- Who will make the decisions about deletion

Provide in **30 days** in electronic format (eg PDF file)

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 notification 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 train showing how consent was given

Getting Consent

Make sure that people 'opt-in' (tick box).

This could look like:

- *I agree for you to use my data for legal reasons associated with running of the club*
- *I agree for you to use my data so that you can provide me with your club's services*
- *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:

- *Updating a form on your website*
- *Logging in to your club management software and changing their preferences*
- *Outlining their request in an email to your club's Data Protection Champion*

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 – Do we require a DPO (Data Protection Officer)

Only required if there is large scale processing of sensitive data so the answer is probably NO for your club

However, every club should have a “Data Protection Champion”

Put reason for not having DPO in Data Protection Policy

Associated GDPR Documentation

Data Protection Policy Template

Privacy Policy Template

Club GDPR Data Processor Agreement Template

Data Controller Processing Logs Questionaire Template

Subject Access Request (SAR) Process Template

Personal Data Security Breach Code of Practice

FOR FURTHER INFORMATION OR TO ASK ANY QUESTIONS PLEASE CONTACT VIVIENNE CLARKE AT +353 1 7163269 OR BY EMAIL ON VIVIENNE.CLARKE@HOCKEY.IE