|  |  |
| --- | --- |
|  | Welsh Chess Union |
| GDPR: Advice to Clubs and Zones |
| Advice to Clubs and Zones on GDPR Compliancy and on how to Audit Data |

|  |  |  |
| --- | --- | --- |
| Author | Version | Date |
| Mark Adams | 0.1 (Draft) | 13th May 2018 |
|  | 1.0 Published Document | 19th May 2018 |
|  | 1.1 Removed reference to encryption. | 19th June 2018 |

|  |
| --- |
|  |

To become GDPR compliant, it is recommended that you complete the following data audit to understand the type of data you hold and the actions you may have to consider. The official legal basis on which clubs and the WCU collects data is that of “legitimate interest”. As a club you are data controllers as you collect membership details. You also act as data processors on behalf of the WCU as you send us member data and results.

What data do you collect?

|  |
| --- |
| (Name, address, email, social media posts, video, photographs) |

Where do you store the data?

|  |
| --- |
| (Documents, databases, backups, email lists, filing cabinet, USB stick) |

How do you protect and document the data you hold?

|  |
| --- |
| (Passwords, encryption, limited access, databases, lock & key) |

How long do you plan to keep the data for?

|  |
| --- |
| (Three Years, Five Years, duration of membership etc…) |

Do you have a function/ reason for every piece of data you collect?

|  |
| --- |
| (Name, Address, Club member details, collected for rating purposes, stored for archival purposes) |

What is the process if someone asks to be removed from your records?

|  |
| --- |
| (Whose responsibility, what records needs to be removed etc...) |

Using the answers to the above questions, add each set of data to the table below and store it formally.

|  |  |
| --- | --- |
| Data Audit Form Asset Detail | |
| Type of Data |  |
| Description of data |  |
| Official responsible |  |
| How consent is collected |  |
| Date of consent to hold data |  |
| 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 |  |

From the audit you will have enough information to provide your members with the following details in your privacy statement:

* The legal basis for collecting data
* What data you will be collecting
* How it will be stored
* Who has access to the data
* Who you will pass it on to and why
* How long you keep the data
* What you do with the data if they object to the way it is used.

The following is a list of guidelines that club and zonal officials need to consider.

* Elect a member who will be the Data Controller.
* Write a privacy statement (in effect a condition of membership) that all members should see and agree to. You can use the WCU statement as a template.
* Only collect data that you will actually use.
* Name those who will have access to data.
* If you have juniors as members, then use the Parental Consent Form on the website (link here).
* If personal data is kept as a hard copy, then it must be securely stored.
* Bear in mind that the passwords must be kept somewhere secure too! If the password is lost, then it is extremely difficult to recover the document without cost. For more information on encryption refer to the ico website: <https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/>.
* Don’t forget, the recipient will need to know the password to read the file.
* DO NOT pass the data on to anyone unless the reason for doing so has been clearly defined and published.
* If you need to send any personal data (i.e. data that can identify a living person) then DO NOT send it in the body of the email, unless the email is encrypted. Send the data as an encrypted and password protected attachment. This is to cover instances where the email ends up with the wrong recipient.
* When sending emails that contain personal data, you must use the BCC field for all recipients. An exception is when emails are passed around committees.