2018

Data Protection Policy

CHESS SCOTLAND
JIM WEBSTER

CHESS SCOTLAND
www.ChessScotland.com

Contents

CHESS SCOTLAND
www.ChessScotland.com

1. Context and Overview

- Policy Prepared by: Jim Webster, President
  Ian Brownlee, Administration Director
- Policy Operational from: Management Board meeting: April 2018
- Document Review Date: 2 Years
-
- Revised for GDPR implementation, May 25th 2018
  (GDPR – General Data Protection Regulation)

1.1. Overview

This document incorporates those changes as required under the General Data Protection Regulation (GDPR) 2018.

The GDPR was adopted in the UK in 2016 and is directly applicable starting on May 2018. This is focused on looking after the privacy and rights of the individual and is based on the premise that data subjects should have knowledge of what data is held about them, and the core information that the Data Protection Act (DPA) did not demand.

The scope of GDPR is far more comprehensive and wide-reaching, meaning that businesses and organisations will need to amend their data protection policies accordingly – or face serious consequences.

Affecting all companies and organisations that collect or process personal information, these new laws are intended to help protect the privacy and rights of individuals, giving data subjects more clearly delineated rights regarding what data is held about them, how it can be used, and when it should be deleted.

The new law reduces the overall number of principles from eight to six, the revamped regulations will be much broader in scope than the existing ones handing the individual greater control over their own personal data and imposing harsh penalties on organisations that fail to comply. These laws apply to any organisation holding data on EU citizens regardless of where they are based.

1.1.1 Key Differences

Chess Scotland is now required to take into consideration the key differences between the old and new rules.

- **Geographic reach and scope**
  GDPR is a binding piece of legislation, which will be legally enforceable as soon as it comes into effect on May 25th, 2018. It will apply to all EU nations and every organisation holding data on EU Citizens.
  Note: Chess Scotland need to ensure that EU individual members of Chess Scotland are included in this legislation.

- **Definition of personal data**
  GDPR expands the definition of "personal data" to include a much wider range of data subject information. GDPR broadens the existing scope to include online identification, location data, genetic data and more.

- **Consent policies**
  This is one of the major differences between DPA and GDPR. Under the DPA data collection does not necessarily require an opt-in, but under GDPR clear privacy notices must be provided to individuals, allowing them to make an informed decision on whether or not to allow their data to be stored and used. This consent can be withdrawn at any time.

- **Data breach policies**
  Under current rules Chess Scotland are under no obligation to report when a data breach occurs although encouraged to do so. This changes with GDPR and breaches must be reported to the relevant authorities within 72 hours of the incident.

- **Accountability**
  GDPR will place a much greater focus on explicit accountability for data protection, placing direct responsibility on Chess Scotland to prove they comply with the principles of the regulation. This means Chess Scotland will need to commit to mandatory activities such as, internal data audits and keeping detailed documentation to avoid falling foul of GDPR rules.

- **Data protection governance**
  GDPR requires that any organisation employing more than 250 people or processing more than 5000 data subject profiles annually will be mandated to appoint a dedicated external Data Protection Officer.

  Chess Scotland falls well out with the boundaries this requirement at this time.

- **Penalties and compensation**
  It is necessary to point out that GDPR will allow individuals to claim compensation for material and non-material damage resulting in data security lapses. Current DPA rules only cover material damage.

1.2. Introduction

Chess Scotland needs to gather and use certain information about individuals

This information can include members, chess organisations and people that Chess Scotland has a relationship with or a need to contact.

This policy describes how this personal data will be collected, handled and stored to meet the requirements of these data protection standards – and to comply within the laws of the United Kingdom.

This data protection policy confirms Chess Scotland

- Complies with data protection law and will follow good practice in using this data
- Protects the rights of its directors and officials
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach.

1.4. Data Protection Law

GDPR describes how organisations – including Chess Scotland – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by six important principles. These say that personal data must:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. Accurate and up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for reason for which the personal data is processed.
6. Processed in a manner that ensures appropriate security of personal data.

2. Risks and Responsibilities

2.1. Scope

This policy applies to:

- Chess Scotland Management Board members
- PVG Lead Signatory
- Membership Secretary

It applies to all data that Chess Scotland holds relating to identifiable individuals. This can include:

- Names of Individuals
- Postal Addresses
- Email addresses
- Telephone numbers
- plus any other information relating to individuals

2.2. Data Protection Risks

This policy helps to protect Chess Scotland from some very real data security risks, including:

- **Breaches of Confidentiality.** For instance, information given out that is unauthorised by Chess Scotland
- **Failing to offer choice.** All individuals should be free to choose how Chess Scotland uses data relating to them.
- **Reputational damage.** Chess Scotland could be compromised should hackers successfully gain access to sensitive data.

2.3. Responsibilities

Every Director and Council member of Chess Scotland has some responsibility for ensuring data is collected, stored and handled appropriately.

Each facility that handles personal data must ensure that it is handled and processed in line in accordance with this policy and data protection principles.

The following officials have key areas of responsibility:

The **Executive Committee** is ultimately responsible for ensuring that Chess Scotland meets its legal obligations.

- The **Administration Director** is responsible for:
    - Keeping the Management Board updated about data protection responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies and up to date for the scheduled review periods.
    - Dealing with requests from individuals to see the data Chess Scotland holds about them (subject access requests)
    - Checking and approving any agreements with affiliates or other third parties that may request Chess Scotland sensitive data.
    - Approving any data protection statements attached to communications such as emails and letters.

- The **Executive Director**, is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services Chess Scotland may consider using to store or process data. (e.g. servers, cloud computing)

3. General Guidelines

- The only people able to access data covered by this policy should be those who require it to perform their responsibilities for Chess Scotland.
- The personal data must be handled in a transparent fair and lawful way. Chess Scotland must make it clear to people how you are going to use their data and why that data is required.
- All data must be used for the explicit purpose it was requested and nothing else. When disclosing what the data is going to be used for upfront this must be specific, explicit and for legitimate purposes.
- Chess Scotland must only request data to carry out the specific purpose stated.
- Chess Scotland may only hold data for a limited period of time (duration of membership for example) for as long as was stated upfront or for as long as it takes to complete the stated task
- Data must not be shared informally. When access to confidential information is required, it must be requested from named individuals.
- All data should be kept secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within Chess Scotland or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

4. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Executive Director.

When data is stored on paper:

Note – these guidelines also apply to data that is usually stored electronically but has been printed out for some reason

- It should be kept in a secure place where unauthorised people cannot see it.
- When not required, the paper or files should be kept under lock and key.
- Data printouts should be shredded and disposed of when no longer required

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be protected by strong passwords that are changed regularly and never shared
- If data is stored on removeable media (CD, DVD, memory devices) these should be kept in a secure location when not in use.
- Chess Scotland must ensure that the personal data held can be easily erased or updated. The data must also be accurate, and Chess Scotland must take steps to ensure its accuracy.
- Data should only be stored on designated drives or servers and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location away from general office space.

- Data should be backed up frequently. Those backups should be tested regularly, in line with standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

5. Data Use

Personal data is of no value to Chess Scotland unless use can be made of it. However, when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

- When working with personal data care must be taken to ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- If someone asks for their data to be updated or removed this must be actioned and across all of Chess Scotland.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.
- Copies of personal data should not be stored on personal computers. Always access and update the central copy of any data.

6. Data Accuracy

The law requires Chess Scotland to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Chess Scotland should put into ensuring its accuracy.

It is the responsibility of all officials who work with data to ensure it is kept accurate and up to date as possible.

- Data will be held in as few places as necessary. There should be no unnecessary additional data sets.
- Officials should take every opportunity to ensure data is updated.
- Chess Scotland will make it easy for data subjects to provide updates of the information Chess Scotland holds about them.
- Data should be updated as soon as inaccuracies are discovered.
  For example: telephone numbers, email addresses.
- Chess Scotland must take steps to ensure the security of the data held. Chess Scotland is responsible for all data held.

7. Access Requests

All individuals who are the subject of personal data held by Chess Scotland are entitled to:

- Ask what information Chess Scotland holds and why.
- Ask how to gain access to it.

- Be informed how to keep it up to date.
- Be informed how Chess Scotland is meeting its data protection obligations.

If an individual contacts Chess Scotland requesting this information, it is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Administration Director (data controller). The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data free of charge and within 30 days

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

8. Disclosing Data for other reasons

In certain circumstances, the DPA allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Chess Scotland will disclose the requested data. However, that data controller will ensure that the request is legitimate, seeking assistance from the Executive Committee and from a legal adviser where necessary,

9. Providing Information

Chess Scotland aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, Chess Scotland has a privacy statement, setting out how data relating to individuals is used by Chess Scotland

[This is available on request. A version is also available on the Chess Scotland website]

CHESS SCOTLAND
www.ChessScotland.com

Appendix 1

Comparison Table DPA v GDPR

For those wondering the differences between the current 'data protection act' (DPA) and the newest about to be implemented being 'GDPR'. This table may be of benefit to you.

DPA (Data Protection Act)	GDPR (General Data Protection Regulation)
The Data Protection Act was developed to give protection and lay down rules about how data about people can be used. The 1998 Act covers information or data stored on a computer or an organised paper filing system about living people.	EU General Data Protection Regulation (GDPR) in Europe, adopted in 2016, will be directly applicable starting on May 25, 2018, and will replace the DPA
Only applies the UK	Applies to the whole of the EU and, crucially, also to any global company which holds data on EU citizens
Enforced by the Information Commissioner's Office (ICO)	Compliance will be monitored by a Supervisory Authority in the UK with each European country having its own SA
Under the current legislation there is no need for any business to have a dedicated DPO	A DPO in some countries will be mandatory for any business or organisation with more than 250 employees
There is no requirement for an organisation to remove all data they hold on an individual	An individual will have the 'Right to erasures - which includes all data including web records with all information being permanently deleted
Privacy Impact Assessment (PIA) are not a legal requirement under DPA but has always been 'championed' by the ICO	PIAs will be mandatory and must be carried out when there is a high risk to the freedoms of the individual. A PIA helps an organisation to ensure they meet an individual's expectation of privacy
Data collection does not necessarily require an opt-in under the current Data Protection Act	The need for consent underpins GDPR. Individuals must opt-in whenever data is collected and there must be clear privacy notices. Those notices must be concise and transparent, and consent must be able to be withdrawn at any time
Direction sets aims and requirements, implemented through national legislation	Regulation is binding for all member states

Personal data and sensitive personal data	In addition, now includes online identifiers, location data, and genetic data
Breach notifications not mandatory for most organisations	Mandatory and within 72 hours
Any person who has material damage is entitled to claim compensation	Any person who has suffered material or non-material damage
Data protection governance down to best endeavour	Recommendation of a data protection officer to be employed from outside the company for organisations with 250+ employees or more than 5,000 subject profiles per annum
Maximum fine is 500,000	Maximum fine 4% of annual turnover or Euro20M whichever is greater
Responsibility rest with the Data Controller	Rests with both the controller and processor with the controller being able to seek damages from the processor
Parental consent for minors not required	Parental consent for minors now required
Accountability is limited	Accountability fully explicit
Subject access requests, £10 per transaction and within 40 days	Free of charge and within 30 days
Data consent free given, specific and informed	Clear affirmation action with the ability to be withdrawn later