Legal note on GDPR compliance for Walking for Health schemes

Background

1.1 The EU General Data Protection Regulation (GDPR) comes into force on 28 May 2018 and represents a significant change to data protection law, coming as it does alongside a new Data Protection Act (currently going through parliament) designed to complement the GDPR and create a new legislative framework for how organisations deal with and protect personal information. A new e - Privacy Directive (which is relevant for marketing) is also expected to come into force shortly. Ramblers is a data controller for the purposes of the current Data Protection Act 1998 and will be so for the purposes of the GDPR and the new Data Protection Act. Ramblers processes a large amount of personal data (including sensitive personal data – called special category data under GDPR) in pursuance of its charitable objects, part of which processing includes that in connection with the Walking for Health programme.

1.2 Walking for Health is an initiative which involves a large number (circa 400) of local schemes across the country. These schemes also are data controllers for their own information and will themselves need to be Data Protection Act and GDPR compliant in how they deal with the personal information they collect, store and process.

1.3 Ramblers intention is to ensure that they and the local schemes do everything required to protect the personal information of those participants in the Walking for Health programme by working together to achieve this. Specifically it is intended that data will be shared between Ramblers and the local schemes on a joint basis with each being a data controller in their own right and for the purposes of the Walking for Health programme acting as data controllers in common. This is because whilst shared data for the Walking for Health programme is used for a shared purpose, some of the information may be used by each controller for other purposes as well.

1.4 In order to ensure the lawfulness of all data sharing, a data sharing agreement based on the joint controller principles referred to above has been produced for the Ramblers and each local group to sign.

1.5 This note provides information and guidance on how Ramblers and local schemes need to work together for GDPR compliance and explains further about what GDPR means and what actions need to be taken by them as data controllers. It is provided by Ramblers to assist local schemes but it is not legal advice and local schemes should seek their own advice on any issues which they remain unclear about or which they have concerns about.

2. **Key terminology for GDPR**

2.1 The following are the key GDPR terms for the purpose of understanding the obligations of data controllers :

2.1.1 personal data – effectively, any information from which a particular living individual can be identified. That identification can either be direct; i.e. based on that information alone; or indirect; i.e. based on that information combined with information in the possession / which may come into the possession of the data controller.

2.1.2 processing – effectively, processing means any operation which is performed on / use made of personal data from collection through to deletion. It includes, for example, organising, storing, adapting, consulting, disclosing and restricting – in brief, it means anything Ramblers or the local schemes do with personal data.

2.1.3 controller – effectively, the person or organisation who (whether alone or with others) decides why personal data is required and directs how it will be processed accordingly.

2.1.4 processor – a person or organisation which processes personal data on the instructions of a controller (i.e. it does not decide the reasons why and the way in which personal data is processed but acts on the instructions of the data controller).

2.1.5 data subject – any living individual in the EU (note: there is no residency requirement) in relation to whom Ramblers or the local schemes processes personal data.

2.1.6 sensitive personal data/ special categories of data – information relating to a person's racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, health, sex life and/or sexual orientation; genetic data and/or biometric data for the purpose of uniquely identifying a living individual.

2.1.7 Data protection officer – under GDPR the DPO role is prescribed and includes specific employment protections, reporting lines and resource access.

2.2 From the point at which Ramblers/ the local group intends to collect personal data from a data subject until that personal data is deleted, Ramblers/ the local group is a data controller for the purposes of the GDPR and must comply with its obligations thereunder.

3. Data protection principles

3.1 In overview, Article 5 of the GDPR sets out the key data protection principles ("Principles) which must be followed by controllers such as Ramblers and the local schemes. In summary, the Principles are as follows:

3.1.1 Principle 1: personal data must be processed fairly, lawfully and in a transparent manner.

3.1.2 Principle 2: personal data can only be collected for specified, explicit and legitimate purposes, and cannot be further processed in a manner incompatible with those purposes.

3.1.3 Principle 3: controllers can only process an amount of personal data limited to what is necessary to the relevant purpose(s).

3.1.4 Principle 4: personal data must be accurate and, where necessary, kept up to date.

3.1.5 Principle 5: personal data cannot be retained for any longer than is necessary in relation to the purpose(s) for which they are processed.

3.1.6 Principle 6: personal data must be processed in a manner which ensures appropriate security.

3.2 Addressing the practical applications of each of the Principles in turn:

Principle 1

3.3 As a basic starting point, the controller has to be up front and clear with data subjects about how, why and for how long they process data subjects' personal data, and it must inform data subjects about the rights they obtain once the controller starts processing their personal data.

3.4 This will largely be catered for by way of a GDPR privacy policy which will need to be developed by each data controller.

3.5 An important element of this requirement is that each controller needs to be able to rely on at least one from an exhaustive list of six "lawful bases" for all of its processing activities. The lawful bases are contained in Article 6 of the GDPR – the relevant bases for the Walking for Health programme will be as follows:

3.5.1 Where the data subject has given their consent to processing – in general, Ramblers/ local schemes should only rely on consent as a sole basis for processing where strictly necessary, because the standard required under Article 4(11) of the GDPR is not straightforward to achieve and because it can be withdrawn at any time, which could cause unwelcome interruption to Ramblers'/ local schemes' processing purposes. The processing activities in relation to which we consider that Ramblers/ local schemes may require consent are:

(a) Any direct communications with individuals about fundraising;

(b) Processing of special categories of data;

(c) Sharing special categories of data with third parties (including each other).

3.5.2 Where processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract – for example, for an employment application.

3.5.3 Where processing is necessary to comply with a legal obligation – for example, if Ramblers is obliged to report a crime to the police.

3.5.4 Where processing is necessary for the purposes of Ramblers'/ local schemes' legitimate interests – this will be the relevant lawful basis for most processing activities. In general, for example provided that an argument can be made that the personal data is reasonably required for the running of the Walking for Health programme or Ramblers/ the local group serving its members, it will be covered by legitimate interests (unless those interests are overridden by the rights and freedoms of data subjects, for example if any processing activity is particularly intrusive or the nature / sensitivity of the personal data means that consent is required for processing).

These bases will be detailed in, and communicated to data subjects via, the privacy policy.

3.6 Otherwise, the general principles of lawfulness and fairness apply throughout the lifecycle of personal data from collection through to deletion.

Principle 2

3.7 In relation to personal data being collected for "specified" and "explicit" purposes, Ramblers and the local schemes have to be up front with data subjects as to why it is necessary for them to process their personal data. This again will be catered for in the privacy policy.

3.8 In relation to those purposes needing to be "legitimate", controllers cannot process personal data for any reason which is, for example, illegal or deceitful, while there needs to be a legitimate reason related to the controller's objectives for processing the personal data.

3.9 In relation to the prohibition on processing personal data for further purpose(s) incompatible with the original processing purpose(s), "incompatibility" is a circumstance-specific concept. If for example Ramblers wants to process personal data it already holds about a data subject for a new, different purposes, it needs to decide whether there is a sufficient link between those purposes to justify not having to give the relevant data subject(s) further information about the reason(s) for that new / different processing (such as to satisfy the requirement of transparency).

Principle 3

3.10 Controllers can only process the amount of personal data which is strictly necessary for the underlying purpose – this will need to be assessed by Ramblers or the local group itself by asking, in relation to each type of processing, "*are we using more personal data than is strictly necessary for this purpose*?" For example, in relation to purposes for which contact details are required, are both email addresses and telephone numbers always required?

3.11 In general, as long as Ramblers and the local schemes can make a reasoned argument why personal data is necessary to achieve the underlying purpose of the processing, there is unlikely to be a breach of Principle 3.

Principle 4

3.12 There is an obligation on a Controller to ensure that the personal data it processes is kept accurate and up to date – it is insufficient to simply expect data subjects to update you.

3.13 Largely, this will be catered for in the privacy policy by offering a simple means (for example, an email address) for data subjects to update Ramblers/ local schemes if the details contained in the personal data change (for example, a new email address, or change of contact name).

3.14 However, all controllers should perform a regular check (for example, an annual email), asking data subjects to confirm that the details in their database remain accurate and up to date.

Principle 5

3.15 Each controller is prohibited from retaining any personal data once the relevant underlying purpose(s) has / have expired.

3.16 Ramblers and local schemes will need to develop an internal data retention policy that ensures, on a practical level, that personal data is not retained once any applicable underlying purpose has expired. We suggest the following approach:

3.16.1 In general, personal data will be retained for six years from the point of collection (this is the usual length of time a data subject has to bring a claim, for example in contract or negligence, against a data controller (and vice versa); therefore a reasonable case can be made that the personal data needs to be retained for the establishment, defence or enforcement of legal claims).

3.16.2 The personal data will be retained longer than six years if still required in connection with the purpose(s) for which it was collected.

3.16.3 The retention policy either needs to be made clear in the privacy policy (a summary is fine), or provided by way of link.

Principle 6

3.17 Data Controllers need to adopt organisational and technical measures to ensure the security of personal data they processes, including protection against unauthorised or unlawful processing and against accidental loss (including dissemination), destruction or damage. The measures that Ramblers/ local schemes need to adopt can be summarised as follows:

3.17.1 Organisational: these include “policy and procedure” measures such as staff training and internal data protection guidelines which ensure that staff understand how to handle personal data in a way that ensure compliance with the GDPR ; and means of ensuring staff compliance with such measures (for example, testing after training).

3.17.2 Technical: these are IT measures and include, for example, appropriate anti-virus software, password-protected wifi and computer access, encryption of personal data when taken offsite via portable storage devices and security of server storage. If there is hard copy storage of personal information this must also be secure – for example locked cabinets with limited key access, locked bags if information is taken off site.

3.18 Each controller needs to adopt measures which are reasonable and proportionate in the circumstances: given that they are processing a comparatively large amount of personal data, and that some of the personal data is of a sensitive nature, Ramblers and the local schemes will be expected to expend a commensurate amount of time and costs in implementing these measures. The data sharing agreement referred to above contains further details of security measures required.

3.19 Part of the data security requirement relates to international transfers of data – we understand that Ramblers/ the local schemes do not send personal data (including sensitive personal data) outside the EEA.

3.20 Finally, an important part of the requirement of organisational measures is a plan to deal with personal data breaches. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (for example, a failure in anti-virus software resulting in a system hack). Ramblers / the local schemes will need to implement a policy which:

3.20.1 ensures that the ICO is notified of the breach without undue delay (no later than 72 hours) after becoming aware of it;

3.20.2 contains plans for recognition, containment and remedy;

3.20.3 ensures that affected data subjects are notified where the breach results in a high risk to their rights of data privacy; and

3.20.4 contains plans for recording the incident and post-incident to discussion to ensure, as far as is reasonably possible, that it does not happen again.

4. Individual rights

4.1 In brief, the GDPR gives data subjects enhanced rights which they can exercise against a data controller. A data controller is required to inform data subjects about these rights and to give them an easy way to exercise them (this should again be catered for in the privacy policy).

4.2 In overview, the rights are as follows:

4.2.1 Right of access: data subjects can write to a data controller to ask for confirmation of what personal data it holds on them and to request a copy of that information (i.e. copies of the relevant documents containing the personal data). This request could be made to Ramblers or the local group as appropriate. Controllers can ask for further information before time starts running for compliance (explained in 4.3 below) if the request does not enable it to identify the relevant data subject or the personal information in question.

4.2.2 Right of erasure: data subjects can ask Ramblers/ local schemes to delete their personal information from its records. The right can only be accessed where the purpose for which the personal data was original processed is no longer applicable (and there are no further applicable, compatible purposes available); where the processing is based on consent and that consent is withdrawn; where an individual has objected (see section 4.2.5 below) and Ramblers/ the local group does not have a legitimate interest to continue processing; and in order to comply with a legal obligation. If validly exercised, Ramblers/ local schemes must delete all records (except to the extent required to ensure that Ramblers/ local schemes can comply with the request, for example by putting a data subject's email on an internal suppression list).

4.2.3 Right of rectification: data subjects can ask Ramblers/ local schemes to update personal data where it is inaccurate, or to check the personal information to verify its accuracy.

4.2.4 Right to restrict processing: data subjects can ask Ramblers/ local schemes to restrict the processing of personal data if there is a disagreement about its accuracy or legitimate usage, pending resolution of that disagreement.

4.2.5 Right to object: data subjects can object to processing where Ramblers/ a local group (i) processes their personal data on the basis of legitimate interests, (ii) uses that personal data for direct marketing or (iii) processes the personal data for statistical purposes. If validly exercised, Ramblers/ a local group must stop processing that personal data unless it can demonstrate compelling legitimate grounds to continue to do so (for example, being essential to its business operations) which override the data subject's rights of data privacy.

4.2.6 Right to data portability: this enables data subjects to ask controllers to send their personal data from one controller to another; or to the data subject him or herself, in a machine readable format. It only applies where processing is carried by automated means (i.e. with no human involvement whatsoever) – we do not consider that this is likely to apply to Ramblers/ local group processing operations.

4.3 Where validly exercised, the requests must be complied with within one month of receipt of the request (or receipt of clarifying information, as applicable). This period can be extended by up to two months, but only in case of complex or numerous requests (the ICO adopts a very strict interpretation of what constitutes complex or numerous).

5. Accountability

5.1 Pursuant to Article 5(2) of the GDPR, data controllers need to be able to demonstrate their compliance with the Principles. In practice, Ramblers/ local schemes will therefore need to keep a written record of all of its processing activities and GDPR compliance (including, for example, consents that have been collected; facilitation of individual rights; discussions relating to data security measures and records of implementation), in case it is challenged by the ICO.

6. Sensitive personal data

6.1 Pursuant to Article 9 of the GDPR, when processing sensitive personal data, a data controller must be able to rely on one from a set of **additional** conditions for processing – the relevant available condition for Ramblers/ local schemes in this regard is the data subject's explicit consent (the use of the word "explicit" would suggest that something additional to the requirements for consent set out in section 8 below is required; for example an explicit recognition of what that data will be used for).

7. Newsletters/ Fundraising/ Marketing

7.1 In overview, concurrent legislation to the GDPR – the Privacy and Electronic Communications Regulations 2003 ("PECR") – prohibits the sending of unsolicited "direct marketing" by electronic channels (email, SMS and telephone where the intended recipient is signed up with the Telephone Preference Service) without prior consent. As mentioned above, there is a new EU privacy directive currently being developed so these regulations are likely to be reviewed once that is in place.

7.2 Direct marketing constitutes any advertising or marketing material, any fundraising material, or any material which, in general, promotes Ramblers/ the local group or its aims and ideals. Ramblers/ the local group should review the materials they send electronically so that the can determine the need for consent.

8. **Consent**

8.1 The requirements for consent pursuant to article 4(11) GDPR are as follows:

8.1.1 Freely given: the consent must not be bundled with another service or set of information (for example, it cannot be buried within a privacy policy) and must be free from any undue pressure or coercion (for example, consent will not be freely given where use of another service depends on providing consent to receive direct marketing).

8.1.2 Specific: the consent must specifically relate to the relevant activity.

8.1.3 Informed: referring to wider relevant information about the use of individuals' personal data, for example by providing a link to the Ramblers/ local group privacy policy so that individuals understand the further implications of providing their personal data.

8.1.4 An unambiguous statement of the data subject's wishes indicated by statement or clear affirmative action: implied consent (for example, not removing a tick from a pre-ticked box) is insufficient – there must be a positive action taken by the data subject to provide his or her consent (for example by ticking a box, or providing their email address).

8.1.5 This can be carried out as part of the registration process (including online) so long as the process ensures any statement of consent is made by affirmative action on the part of the individual registering.

9. **Further information**

9.1 The following further information may be of use to local schemes still working on their GDPR compliance:

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/#draft