IAM RoadSmart

GDPR and Data Management Guidelines for Groups

IAM RoadSmart

GDPR and Data Management Guidelines for Groups

Version	V1.04
Author/creator	Peter Serhatlic
Authoriser	EDT
Owner/department	EDT
Document classification	Restricted
Document Status	Released

History and revisions

Version	Created by	Document Classification	Revision History	Date Published
V 1.0	Peter Serhatlic	Restricted	Initial Draft	04/04/2018
V1.01	Pat Doughty	Restricted	First Amends	3 April 2018
V1.02	Pat Doughty	Restricted	Appendices added, plus quick start checklist	4 April 2018
V1.03	Pat Doughty	Restricted	Factual Updates made following review by N Harris	12 April 2018
V1.04	Richard Gladman	Restricted	Grammar and punctuation (proofreading document)	17/04/2018

Authorisation

GDPR Policies are authorised by EDT as Sponsors and this is evidenced by the CEO confirming EDT approval.

Version	Authorised by	Department	Date
V1.03	Sarah Sillars	CEO	12/04/2018
V1.04	Sarah Sillars	CEO	17/04/2018

Table of Contents

1.0 Introduction and Purpose

The GDPR (General Data Protection Regulation) is EU legislation. Whilst the UK remains in the European Union, the GDPR applies automatically and IAM RoadSmart will have to comply with it by 25th May 2018 or show that an implementation plan is in place.

Post Brexit the UK would still need its own data protection legislation such as GDPR or equivalent.

The GDPR is more formulaic than the UK data protection legislation has been up to now. The GDPR does not just lay down the principles of what needs to be achieved but in many cases says exactly what you have to do to be compliant. This makes it seem very new and challenging but many of the new practices just reflect what has been best practice (but not law) up to now.

The main new feature of data protection under the GDPR is an accountability principle, meaning that an organisation not only has to comply but it has to be able to demonstrate that it complies.

The main aim of this policy is to enable IAM RoadSmart Groups to manage their data effectively and in compliance with data protection and other regulations. As an organisation we collect, share, hold, store and create significant amounts of data and information.

This policy provides a framework of retention and disposal of categories of information and documents, thereby ensuring both IAM RoadSmart and IAM RoadSmart affiliated groups meet our obligations in relation data management.

The implementation of these guidelines demonstrates the commitment to the principles of data protection, including the principle that information is only to be retained for as long as necessary for the purpose concerned.

These guidelines propose the creation of a new role within Groups, of the Group Data Manager. The Role Profile for this post is shown at Appendix i.

This is a valuable specific role within groups, and it is recommended it should be occupied by an Officer/Committee member of the Group.

If this role is not implemented, then responsibility for the overall Group management of GDPR will fall to the Trustees of the Group, as noted on the Charity Commission web-site for each Group.

Note: - IAM RoadSmart will be requesting that each group completes the Group Declaration Form (appendix v) to confirm receipt and implementation of the guidelines.

2.0 Data Processor Checklist

The purpose of this section is to make you aware as Groups, of the relationship that will exist between the Data Controller (IAM RoadSmart) and the Processor (IAM RoadSmart groups).

On the occasions when Groups collect Data from its Members, Associates, and Affiliates, that they require to function, the group becomes the data controller in relation to that data.

In simple terms, when IAM RoadSmart (Data Controller) passes to a Group details of a new Associate allocated to that Group,(Data Processor) those details can only be used for the purpose of delivering Driver or Rider Training.

This checklist should be used whenever you are using a third party to deal with personal data on your behalf. You will continue to be responsible for the information, and the third party will be restricted to doing only what you tell them. They will have no right to keep or use the information for any of their own purposes. You will be the Data Controller, and the third party is the Data Processor.

If the Group then wish to use these details as a contact for example, for informing of Social Functions, then the Group will need to enter into a contract with the individual for this purpose. (An example contract can be found in Appendix iii. The aspect of contracts and permissions is covered in greater detail in Section 4: Data Retention Policy.

The following outlines the prescriptive tone of the Legislation, and the responsibilities it places on Data Controllers and Processors, however later in this document we outline the guidelines for groups to implement and to ensure compliance with the new legislation

Data Controllers are required to use only Data Processors providing sufficient guarantees to implement appropriate data protection measures and ensure compliance. Adherence of a Processor to an approved code of conduct or approved certification assist's in demonstrating that sufficient guarantees exist. We recommend that the Processor's adherence to an approved code of conduct or approved certification should be recited in the agreement the controller has with the Processor.

To comply with the legislation, your agreement with the Processor must:

- Be in writing:
- Contain the following information on the processing:
    - its subject matter and duration;
    - the nature and purpose of the processing;
    - the type of personal data;
    - the categories of individuals who are the data subjects.
- Expressly state that the Processor can only act on your instructions as the Controller.
- Require the Processor to impose a duty of confidentiality on relevant staff.
- Require the Processor to implement relevant security measures to protect the data. You can specify what those measures are, and what you impose will depend upon the type and sensitivity of the information.
- Require the Processor to seek your prior written permission as Controller to engage a sub-contractor.
- Require the Processor to make all necessary arrangements to ensure that as the Controller you can respect the rights of the individuals under data protection law. As an example, The Processor must be required to make available any personal data should an individual make a Subject Access Request; must be able to delete or rectify data if necessary and must enable data portability where applicable.
- Require the Data Processor to have in place the necessary means of assisting you as the Controller to meet your obligations under data protection law. This includes ensuring security of data, co-

operating in relation to your notification of breaches to the Information Commissioner's Office and data subjects, and with preparation of data protection impact assessments.

- Require the Processor to assist you as the Controller in meeting any obligations imposed by the Information Commissioner's Office, by allowing access to information, and details of activities and systems if and when required.
- Require the Processor to delete or return the data at the end of the contract. The choice of whether the data is returned or deleted is your decision as the Controller.
- Require the Processor to provide you with all necessary information regarding processing activities to demonstrate compliance – including security measures taken, disclosures made, what has been done to the information plus anything else you need to know as Controller to allow the processing to be audited.
- Provide that any legal requirements that the Processor is subject to which may require the disclosure of the personal data (such as Freedom of Information) should be notified to you as the Controller in advance, where possible.

Checklist

☐ Agreement is in writing under law of England and Wales [or law of EU or other member state]
☐ Names of Processor and Controller details
☐ Details of the processing project, its purpose, subject matter and duration
☐ Processor can only act on instructions of Controller
☐ Duty of confidentiality for Processor's staff
☐ Processor to implement necessary security measures
☐ Only sub-contract with Controller's permission
☐ Make arrangements which allow Controller to respect rights of data subjects
☐ Assist the Controller with security and other data protection compliance
☐ Assist the Controller with Information Commissioner requirements
☐ Delete or return data at the end of the contract
☐ Details of processing activities to be made available to Controller
☐ Any legal requirements for disclosure to third party by Processor to be notified

3.0 Privacy Policy

The privacy policy – also known as an Information Notice, or Privacy Notice - is the information that you are REQUIRED to give to individuals about whom you hold personal data.

Slightly different rules apply to information that you are given by third parties, as opposed to information you have obtained yourself, and this is explained further below.

By way of an example:

As a Group the information you will be given by a third party, (IAM RoadSmart) – will be information that you need to deliver Driver/Rider Training. This will be:

- Name
- Address
- Year of Birth
- Contact details.

Please note, this is all the information that is required. Importantly, this data is given by the individual for the sole purpose of Driver/Rider training.

If you wish to then use this for group circulars, Social Invites, Newsletters, you will require to enter into a contract (see appendix iii) with the individual for this, For further detail refer to:-

Section 4 - Data Retention Policy and Appendix (iii) which is the IAM RoadSmart format to be used.

There is no requirement or purpose in collecting the following:

- Driving Licence numbers
- Vehicle registration, make or model
- Driving Conviction Information etc.

If these are held, then steps must be taken to securely destroy this information immediately.

Note: - For the associate details, you will be classified as a Processor.

Should you then, as a Group for example collect bank account details to collect group subscriptions by Direct Debit, then for this information you will become a Controller.

The IAM RoadSmart GDPR guidelines outlines the necessary steps required to manage this information.

4.0 Data Retention Policy

Organisations collect, hold and store a vast amount of data and information. This section will provide an in-sight into the management of this data.

The key principle behind Data Retention is that Information is only to be retained for as long as necessary for the purpose concerned. Provided below is an example of a suggested table you keep to monitor the data and information you, importantly why it is kept, and the period it is kept for.

Certain data you will need to be kept under statute, such as annual accounts and meetings of minutes.

Appendix iv provides a table of Legal requirements to help you with this process

Advice on the destruction of documents and data, can be found in section 5 of this document.

The Group Data Manager or nominated trustee will be responsible within the Group for all data matters, which will include

- The recording of the data collection
- Its storage
- Its applicability
- Its security
- Giving advice on its relevance
- Its destruction

A Data Retention Policy Checklist is given at Appendix ii

4.1 Suggested Table Format for listing retained data

Data	Contract	Notes
Name	✓	Contracted by IAM RoadSmart at point of purchase
Address	✓	Contracted by IAM RoadSmart at point of purchase
Gender identifier	✓	Contracted by IAM RoadSmart at point of purchase
Year of Birth	✓	Contracted by IAM RoadSmart at point of purchase
Post Code	✓	Contracted by IAM RoadSmart at point of purchase
E-mail address	✓	Contracted by IAM RoadSmart at point of purchase
Telephone	✓	Contracted by IAM RoadSmart at point of purchase
Next of Kin details (NoK)	✓	NoK has to give consent & confirmed in a declaration signed by The Associate
'Run sheets' Kept by Associate Kept by Group Copy each Membership by Groups Sign Off (MBGSO)	✓ ✓ ✓	For the purpose of the training course, it is acceptable for Groups to be able to have sight of the Run Sheets, to monitor and evaluate training. Contract for this will be part of the purchase of the Course. This then requires secure storage and access **This will also include video and audio footage of Training**

On completion of the Course, or abandonment of the training, the Run Sheets will revert to the Associate, and the Group confidentially destroy their copies, or return them to the Associate.

Post Associate Group Involvement.

Data	Contract	Notes
Personal Details as above	✓	Once an associate either becomes a full member, or fails, or doesn't complete the course, and does not renew the Course, then the original contract ceases. A new group contract will then need to be issued by the Group for inclusion on Group circulars, publications and contact with the Group. This will then require secure storage and access facilities This will require the issue of the Group Contract to all group members on an annual basis when membership fees are collected
Bank Account details	✓	For D/D collections – Securely stored and accessible only by authorised Trustees e.g. Treasurer
Social Media feeds	✓	Inclusion in this type of activity requires covering by issuing the group contract. Or if available to public through sharing platforms the identities of members should be invisible This will require the issue of the Group Contract to all group members on an annual basis when membership fees are collected
Observer Training	✓	Contract for inclusion in IMI registration will be required through the issue of the group contract. During training the LOA will need to complete a portfolio of evidence – for LO qualification – for submission to IMI. On completion of training, then it is good practice to engage with CPD, so the initial consent needs to reflect this. The NO process slightly different whereby info is stored on DTE, shared with IMI, shared with a Group nominated person and individual – consent needs to reflect this. If an Observer ceases in the role, data held should be cleansed and a skeleton record indicating the IMI qualification identifier replacing the training record, any resumption in the future can be accessed by the identifier. IAM RoadSmart has in place data sharing agreement with IMI Groups should not retain Training records of non-active Observers.
Lapsed or deceased members		Groups cannot hold any data on non-members, personal data including run sheets or training sheets have to be returned and/or securely destroyed
Data Privacy & Retention		Groups have to securely protect data, and advise members of the need to protect data
Data questions		Groups need to identify who the Group Data Manager is within the Group (good practice maybe to have this as a committee role). To answer Data questions from members
Data cleansing		Groups must have a scheduled data cleansing programme to ensure Data held is relevant to their purpose, accurate, and valid

4.2 Retention Period

This is the part of the policy that you will need to comply with according to your specific needs. List all data types utilised under each functional heading and complete the relevant retention information. The table below outlines examples of the types of documents, and the recommended retention periods. As long as you can justify the length of time, you can choose how long to keep records, and you can amend this policy at any time.

It's important, data should never be deliberately deleted or destroy anything in order to avoid disclosure in response to a Subject Access Request

RECORDS HELD (type of data)	**REASON FOR RECORD (the purpose or use of the data)**	**RETENTION PERIOD (timescale in years)**	**ACTION FOLLOWING RETENTION**	**ACTION COMPLIES WITH**
Full Group members. Name; gender; year of birth; address; E-mail: telephone; Bank Account details when D/D is used to collect payment	Group demographic; Marketing, Social Contact; official group business Payment of Group funds	Permanent while the person remains a Group member	If a member leaves the Group, all data held to be destroyed Any records in existence relating to lapsed members to be destroyed. All records to be held electronically Computers, tablets, and Smart Phones used to keep data on to be password protected No paper records kept	GDPR Guidelines. IAM Policy
Associates: Name; address; Year of Birth; e-mail; telephone Next of Kin (NoK)details Portfolio of evidence regarding course progression	Corporate demographic of age Marketing Contact details Associate to inform NoK that details held Run sheets to be retained by Associate Membership by Group Sign Off (MBGSO) Run Sheets	Once converted to full member, Data held as above.	If associate does not continue to full membership, all data to be cleansed and any records kept to be handed back to associate Storage of data as above	GDPR Guidelines IAM Policy
Group Meetings and accounts	Legal requirement	Ten years	Destroyed	Charities Act 2011 Companies Act 2006
Observers; Training records (inc Video) Personal details as at Group members CPD attendance Portfolio of evidence Associate details	Contact associates Proof of progression of learning as an Observer	While active in role	Destroyed	IAM Policy GDPR Guidelines

4.3 Handling and Security of Data

GDPR imposes greater restrictions on Organisations with regard to the Data they can legitimately collect and use.

The previous sections have identified the type of Data that is required for a Group to function.

There is no requirement for Groups to hold data that they have accumulated in the past.

Therefore part of this legislation and process will call for data to be cleansed to comply with the GDPR and IAM RoadSmart policy. Any data in excess of the identified data must be destroyed immediately.

Circulation lists that are used to keep your members informed of events, and the use of Social media platforms to publicise their Group activities and achievements, under the new legislation now require a contract with your existing members utilising the form outlined in Appendix iii

It is also necessary to renew this contract on an annual basis, by issuing it with your membership fee collection.

It should also be noted that the contract must provide the member with the option to withdraw from the contract at any time.

All data that you hold must be securely stored and protected. Documents held electronically (preferred method) must be password protected with access rights granted to Group people who have a necessary and legitimate purpose for access.

This will be the responsibility of the Group Data Manager or nominated trustee, who will also be responsible for providing individuals with their right to view what data is held by you, on them.

It is recommended that groups register as a Tier 1 category within the GDPR Guidelines as a Charity, there will be an annual £40.00 fee payable to the Information Commissioners Office

Visit the link https://ico.org.uk/for-organisations/register/ to register as an organisation and pay

Summary of Contracts required for the use of Personal Data

levels of permissions required to use Personal data	An Associate is allocated to a Group, or recruited by a Group. At point of purchase a contract is entered for the purpose of delivering the Course only. Inclusion into Group circulars and activities will require seperate contract from the group as recommended in Appendix iii
	The course is completed, and the associate becomes a full member. If the Group practice is to collect membership fees by D/D then a seperate permission wil be required If the course is abandoned, or the associate is unsuccesful at test and does not renew the course, then all data held regarding the associate, must be returned to them and/or destroyed.
	Existing Group members must now be provided with a contract from the group to continue to use their data for Group circulars, D/D collections, or for Observer purposes. This contract should be renewed every twelve months as appendix iii

5.0 Destruction of Data

The GDPR legislation now puts a responsibility on the group to securely manage data held

While strict emphasis has been placed on the data that can be collected and its associated use, there is equal emphasis placed on how to destroy data when its relevancy has expired.

In order to comply with the new regulation all Groups should firstly obtain a clear understanding of where all their data resides. Under this regulation, once data exceeds the retention period, or an individual exercises the right to be forgotten, data should be deleted in accordance with your policies. Therefore we request that each Group assesses their disposal/deletion procedures and make the appropriate updates

Secure waste (physical documents/data)

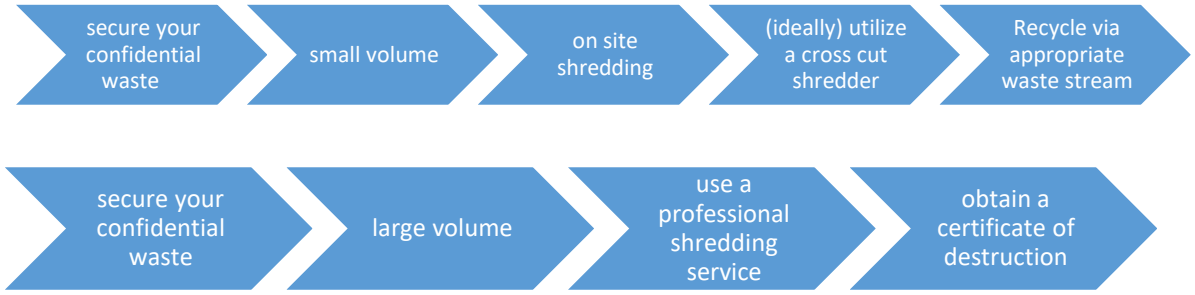
There are various ways you could dispose of secure waste, locked bin, tied up sacks etc. The fundamental part is to ensure that no person has access to the secure waste.

Ensuring your confidential waste is disposed of securely is vital to protect your group;

Points to take into consideration:

- Firstly ensure sensitive documents are not left unsecured
- Discarding documents into waste paper bins is not secure
- Depositing documents into locked containers (bins) is the safest option

Chain of care:



WEEE waste (Waste Electronic Electrical Equipment) directive (incl. ink cartridges)

This is a regulation aimed to separate electronic equipment from municipal waste in order to ensure that electronic items such as copiers, fax machines and printers are correctly disposed of and where possible recycled. This includes removing all confidential data held on electrical devices.

Chain of care

For a more detailed understanding of the duty of care with regards to waste use the following links:

HSE: http://www.hse.gov.uk/waste/waste-electrical.htm

Gov website: http://www.legislation.gov.uk/uksi/1991/2839/contents/made

Destruction of Electronically Held Data.

To cleanse data off of computers, mass storage disks, memory sticks etc., so that the data cannot not be stolen or utilised by others, the simple activity of deleting the data doesn't actually delete but merely hides it from immediate view, therefore other measures may need to be used.

Different technology and scenarios call for different tools. It's important to seek additional guidance for and advice on the best methods. One article that we recommend to read can be found at the following link. **(Reference from PC World)**

https://www.pcworld.com/article/261702/how_to_securely_erase_your_hard_drive.html

Appendix i

Role Profile – Group Data Manager

Job Summary

- The Group Data Manager is part of the Group Committee
- To ensure the Group operates in accordance with GDPR and IAM RoadSmart guidelines

Key Responsibilities

- To manage data collected, used, stored, retained and destroyed in line with GDPR and IAM RoadSmart guidelines

Key Tasks

To provide guidance to data holders in line with GDPR and IAM RoadSmart guidelines

To ensure records of contract and all data used by the group is:-

- Accurate
- Securely Held
- Used in accordance with GDPR Guidelines
- Retained
- Securely Destroyed

Report any breaches in data protection to IAM RoadSmart and the appropriate authority

Ensure the correct GDPR notices are included in all group communication to associates/members.

Manage any request of the option to withdraw by associates/members

To review relevance of historical data

Key Skills

Sound knowledge of GDPR and IAM RoadSmart Guidelines

Good interpersonal skills

IT literate, adept in use of DTE, internet, and Email skills

Further information on GDPR and Data Protection can be found at: - https://ico.org.uk/

Appendix ii

Data Retention Checklist (reference ICO.org.uk)

The GDPR sets out additional requirements around retention of personal data compared to the Data Protection Directive. Given that breach of these provisions can lead to the imposition of considerable fines, data retention is not simply a matter for IT and administration, but a business consideration with potentially significant financial impact if you don't get it right. This checklist sets out the key issues that a group should consider when implementing a data retention policy.

Data storage

First of all, it is important to have an overview of where personal data is stored in your group. This may include:

- own servers;
- third party servers;
- email accounts;
- desktops;
- employee-owned device (Bring your own device(BYOD));
- backup storage; and/or
- paper files.

General retention periods

Generally personal data should only be retained for as long as necessary. The retention periods can differ based on the type of data processed, the purpose of processing or other factors. Issues to consider include:

- Whether any legal requirements apply for the retention of any particular data. For example:
  - Trade law;
  - Tax law;
  - Employment law;
  - Administrative law;
  - Regulations regarding certain professions, e.g. medical.
- In the absence of any legal requirements, personal data may only be retained as long as necessary for the purpose of processing. This means data is to be deleted e.g. when:
  - the data subject has withdrawn consent to processing;
  - a contract has been performed or cannot be performed anymore; or
  - the data is no longer up to date.
- Has the data subject requested the erasure of data or the restriction of processing?
- Is the retention still necessary for the original purpose of processing?
- Exceptions may apply to the processing for historical, statistical or scientific purposes.

During the retention period

- Establish periodical reviews of data retained.
- Establish and verify retention periods for data considering the following categories:
  - the requirements of your business;
  - type of personal data;
  - purpose of processing;
  - lawful grounds for processing; and
  - categories of data subjects
- If precise retention periods cannot be established, identify criteria by which the period can be determined.
- Establish periodical reviews of data retained.

Expiration of the retention period

After the expiration of the applicable retention period personal data does not necessarily have to be completely erased. It is sufficient to anonymise the data. This may, for example, be achieved by means of:

1. erasure of the unique identifiers which allow the allocation of a data set to a unique person;
2. erasure of single pieces of information that identify the data subject (whether alone or in combination with other pieces of information);
3. separation of personal data from non-identifying information (e.g. an order number from the customer's name and address); or
4. aggregation of personal data in a way that no allocation to any individual is possible.

In some cases, no action will be required if data cannot be allocated to an identifiable person at the end of the retention period, for example, because:

- the pool of data has grown so much that personal identification is not possible based on the information retained; or
- the identifying data has already been deleted.

Information obligations

In addition to other information obligations, in the context of data retention data subjects must be informed of:

- the retention period;
- if no fixed retention period can be provided – the criteria used to determine that period; and
- the new retention period if the purpose of processing has changed after personal data has been obtained.

Appendix iii

Group Required Contract Statement to Members

Here at GROUP-NAME we would like to thank you for becoming/renewing your membership with us, as part of your membership contract with us, we will contact you with information on training, committee, and social events, together newsletters/magazines relating to the group and Road Safety.

Pictures, videos and written updates of GROUP-NAME events such as training, committee and social events at which you may be in attendance or referred to, will also be regularly published on Social media sites such as Facebook, Twitter etc, group newsletters/magazines and group related websites.

GROUP-NAME also share your information with The Institute of Advanced Motorists in order to administer membership activities.

Option to Withdraw from the above

You have the right to withdraw from receiving or participating in any of the above, by contacting ***GROUP-NAME.***

I do not wish to:-

☐ receive information on training, committee, and social events, together newsletters/magazines relating to the group and Road Safety.

☐ to appear in or be referred to in or on any group social media sites such as Facebook, Twitter etc, group newsletters/magazines and group related websites.

Signature: _____

Name (in capitals): _____

Date: _____

Membership Number _____

Please notify the ***GROUP-NAME*** by email to **Local Group Mailing Address Here** or letter to:-

Group Secretary

GROUP-NAME

1 the Street,

Town

Post Code

Appendix iv

Statutory and Legal Requirements for keeping certain Data

This is for reference when compiling your retention period framework in Section 2. It covers the main categories of documents with a legal or commercial requirement to keep them for a set period, relevant to charities generally. There may be other requirements in relation to the sectors or areas of activity you operate in.

DOCUMENT TYPE	LEGISLATION/REASONS FOR RETENTION	REQUIREMENT
CORPORATE/CONSTITUTIONAL RECORDS		
Royal Charter/Bylaws/Trust Deed/unincorporated association constitution	Charities Act 2011	Permanent
Trustee/director minutes of meetings and written resolutions	Companies Act 2006 Charities Act 2011 CIO (General) Regulations 2012	Recommended at least 10 years
Members' meetings etc Minutes/resolutions	Companies Act 2006 Charities Act 2011 CIO (General) Regulations 2012	Recommended at least 10 years
TAX AND FINANCE		
Annual accounts and review (including transferred records on amalgamation)	Companies Act 2006 Charities Act 2011 CIO (General) Regulations 2012	Minimum 6 years Recommended: permanent record
Tax and accounting records	Finance Act 1998 Taxes Management Act 1970	6 years from end of relevant tax year
Information relevant for VAT purposes	Finance Act 1998 and HMRC Notice 700/21	Minimum 6 years from end of relevant period
Banking records/receipts book/sales ledger	Companies Act 2006 Charities Act 2011	6 years from transaction
Deed of covenant/Gift Aid declarations and correspondence re donations	As part of tax records	6 years after last payment or 12 years if payments are outstanding or dispute over deed
Legacies – correspondence and financial records		6 years after completion of estate administration

Appendix v

General Data Protection Regulation (GDPR) Guidelines Receipt and Implementation Declaration

To : Head of Field Service Delivery
IAM RoadSmart
1 Albany Place
Welwyn Garden City
Hertfordshire
AL7 3BT

Email:- Amanda.smith@iam.org.uk

Group Name hereby declare that :

- □ We have received the IAM RoadSmart guidelines regarding the management of personal data in relation to members of IAM RoadSmart and the group
- □ We understand the requirements to securely destroy all historical data relating to non-active members, no matter which format it is held in such as digital or hard copy etc.
- □ We understand the recommended types of data that can now be held and the relevant retention periods.
- □ We understand the necessary statement that is required to be issued to all group members regarding communications and activities that may receive or be part of.
- □ We will implement the guidelines as recommended and gain further clarification or advice on any items that we are not sure of.
- □ We have reviewed the requirement of registering with the Information Commissioner's Office.

We also acknowledge that we shall make another declaration to state any change in any matter contained in this declaration immediately before the change occurs

Group Chair	**Group Secretary**
Signature :	Signature :
Name :	Name :
Date :	Date :

Note :

(a) Please put a "✓" in the appropriate box

Appendix vi

Quick Start Check List

What to do	Assigned to	Date Completed
1. Appoint a Group Data Manager or Trustee to fulfil the role		
2. Create a full inventory of all Group members that hold data I. Type of data II. Media held on (Electronic, Hardcopy etc.) III. Establish whether its secure IV. Establish whether its relevant to their role in the group V. Establish its use VI. Establish its age		
3. Review the types of data held, and align with guidelines as appendix ii		
4. Implement a data security protocol for all data shared with members of the group I. Lock Data II. Password protect III. Enforce its only to be used for the purpose created and cannot be shared (Privacy Policy)		
5. Implement the member contract with all existing members		
6. Implement the contract with all new associates		
7. Cleanse all historic data		
8. Organise the secure destruction of all historic data held on members		
9. Implement process to ensure that members that request to withdraw from the contract, have their requirements met, in all sets of data held.		
10. Review the requirement of registering with the Information Commissioner's Office.		

1 Albany Place
Hyde Way
Welwyn Garden City
AL7 3BT

Registered in England and Wales 562530
Registered charity number 249002 (England and Wales) SC041201 (Scotland)

www.iamroadsmart.com