

Lions Clubs International

Multiple District 105

Heads-up to Club

(v 0.2)



DOCUMENT INFORMATION

Master Location	:	C:\Users\David\Documents\Lions\Multiple District 105\Data Protection\European Data Protection Regulation\Forthcoming changes\GDPR - Heads-up to Clubs.docx
File Name	:	GDPR - Heads-up to Clubs
Distribution		

VERSION HISTORY

Version Number	Date	Details of Changes included in Update	Author(s)
0.1	13-02-2018	Initial draft document	David Colville
0.2	26-02-2018	Inserting Section 4.2 'Proforma Consent Examples'; deleting Section 5.2; rewrite Section 9, changing heading & content; and inserting 10.1, 10.2 & 10.3.	David Colville

Table of Contents

1	Headline impacts of General Data Protection Regulation	4
1.1	Documents available on MD105 web site	4
1.2	Documents in progress – March.....	5
2	Privacy Principles	5
2.1	Lawfulness, fairness & transparency	5
2.2	Purpose limitation	5
2.3	Data minimisation.....	5
2.4	Accuracy	6
2.5	Storage limitation	6
2.6	Integrity & confidentiality.....	6
2.7	Accountability & compliance	6
3	Conduct an inventory & data flow audit	6
4	Consent	7
4.1	Children’s Consent.....	8
4.2	Proforma Consent Examples.....	9
5	Fund Raising	10
5.1	Example: include this statement in an application form.....	12
6	Subject Access Request.....	12
7	Data subject’s rights	12
8	Develop operational policies, procedures & processes.....	14
9	Web Site(s) & Cookies	14
9.1	Privacy& Electronic Communications Regulations (PECR).....	14
10	Member awareness e-learning courses.....	16
10.1	Video ‘What is Privacy?’	16
10.2	Video ‘What is Data Protection?’	16
10.3	Video ‘What is Meta Data?’	16
11	Useful links.....	16

1 **Headline impacts of General Data Protection Regulation**

- New accountability requirement means organisations are now required, not only to comply with the new law, but to demonstrate that they comply with the new law. In particular, there is a requirement to keep records of data processing activities.
- Significantly increased penalties possible for *any* breach of the Regulation – not just data breaches.
- Legal requirement for personal data breach notification to the ICO within 72 hours where risk to data subjects.
- Removal of charges, in most cases, for providing copies of records to club members or members of the public who make a subject access request.
- Requirement to keep records of data processing activities.
- Data protection issues must be addressed in all information processes at an early stage.
- Specific requirements for transparency and the provision of information to data subjects about how their information is used.
- Tighter rules on consent where this is used as a basis for lawful processing (there are alternatives to consent).

1.1 **Documents available on MD105 web site**

(<http://lionsclubs.co/MemberArea/?p=252>)

GDPR - Forthcoming changes to Data Protection (24/07/2017)
GDPR - Consent Overview (24/07/2017)
GDPR – Proforma Club Consent Form (Advertise Event)
GDPR – Proforma Club Consent Form (Friends of Club)
GDPR – Proforma Club Member's Consent Form (Publish Directory)
GDPR – Proforma Club Member's Consent Form (Email Distribution)
GDPR - Consent Procedure
GDPR - Data Subject Consent Form (Template)
GDPR - Withdrawal of Consent Procedure
GDPR - Privacy Notice (Draft)
GDPR - Privacy Procedure
GDPR - Privacy Notice Register
GDPR - Web Site Privacy Statement (24/07/2017)
GDPR - Training Policy
GDPR - Complaints Procedure
GDPR - Subject Access Request Procedure
GDPR - Subject Access Request Application Form

GDPR - Retention & Disposal Schedule

GDPR - Fund Raising & Data Protection Guidance

GDPR – Role of the Data Protection Office (28/08/2017)

GDPR - Transfer of Personal Data to Third Countries or International Organisations Procedure

GDPR - Glossary of Terms (24/07/2017)

1.2 Documents in progress – March

- GDPR – Data Protection Policy Statement
- GDPR – Data Portability Procedure
- GDPR – Guide to Retention of Records
- GDPR – Internal Breach Register
- GDPR – Managing Sub Contract Processing
- GDPR – Parental Consent Form
- GDPR – Parent Consent Withdrawal Form
- GDPR – Personal Data Breach Notification Procedure
- GDPR – Retention & Disposal Schedule
- GDPR – Subject Access Request Record

2 Privacy Principles

GDPR lays down a set of data protection principles to guide how organisations manage personal data.

2.1 Lawfulness, fairness & transparency

Personal data must be processed lawfully, fairly, and ***in a transparent manner in relation to the data subject***. The grounds for processing personal data under the GDPR broadly replicate those under the current legislation. The data subject must be told what process will occur (transparent); the processing must match the description (fair); and the processing must be for one of the purposes specified in GDPR (lawful). There are new limitations on the use of consent and the processing of children’s data.

2.2 Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Privacy notices, terms & conditions, and consent forms should provide the data subject with unambiguous information about the extent of the processing involved.

2.3 Data minimisation

Personal data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed. You should hold no more data beyond what is strictly required.

2.4 Accuracy

Personal data must be accurate and, where necessary, kept up to date.

2.5 Storage limitation

Personal data must be kept *in a form which permits identification of data subjects* for no longer than is necessary for the purposes for which the personal data are processed.

2.6 Integrity & confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.7 Accountability & compliance

You are responsible for ensuring compliance with the previous six principles and for being able to demonstrate compliance. You need to ensure that the data protection principles are met wherever the personal data goes – e.g. external processing. Essentially, GDPR clarifies who is responsible for data protection and privacy at each stage of data processing.

3 Conduct an inventory & data flow audit

A fundamental part of our GDPR compliance project is understanding what personal information you are collecting and processing. A lack of understanding will make it difficult to ensure that your club's data processing activities comply with the new obligations set out in the GDPR. The key to GDPR, and every other regulation in this space, is a sound approach to data protection across the organisation. **It's not a security or a technology problem, but a holistic business problem.**

- Assess the categories of data held, where it comes from and the lawful basis for your processing.
- Map data flows into, within and from your club.
- Use the data map to identify the risks in your data processing activities and whether a data protection impact assessment (DPIA) is needed.

Information you hold - A fundamental part of GDPR compliance work is understanding what personal information club members are collecting and processing.

- **the entry point:** what personal data they collect, where and who it comes from, how it comes into our organisation and why they are receiving it?

- **the process:** where the data goes and what happens to it while it is in your organisation – where and how is it stored, who has access to it and why (is anything superfluous)?
- **the inputs:** what additional data is added from internal and external sources to the data they receive, who does it and why? Is any of this additional data inferred through profiling or similar means?
- **the outputs:** what will be produced with the data in terms of reports and other outputs?
- **the exit point:** when and how is the data deleted or exported from the organisation? If it is exported to a third party – who are they, what is the basis for the data being exported, and how and why will the third-party process it?

4 Consent

The GDPR defines consent as ***“any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”***.

However, this definition is only the starting point for the GDPR standard of consent. Several new provisions on consent contain more detailed requirements. In particular, Article 7 sets out various conditions for consent, with specific provisions on keeping records of consent, clarity and prominence of consent requests, the right to withdraw consent, and avoiding making consent a condition of a contract.

Under GDPR, consent must be “freely given, specific, informed and an unambiguous indication of the subject’s wishes by which he or she, by a statement of clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. ***Essentially, this requires subjects’ must “opt-in” rather than “opt out”*** - the GDPR specifically bans pre-ticked “opt-in” boxes.

Consent is no longer permitted to be a pre-condition to signing up to a service unless necessary as this would not be full consent, and must now also name the parties who will be relying on the consent and using the data, and where possible there should be options for the individual to consent to different types of data processing.

The key new points are as follows:

- **Unbundled:** consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.

- **Active opt-in:** pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods (e.g. a binary choice given equal prominence).
- **Granular:** give granular options to consent separately to different types of processing wherever appropriate.
- **Named:** name your organisation and any third parties who will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR.
- **Documented:** keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.
- **Easy to withdraw:** tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means we will need to have simple and effective withdrawal mechanisms in place.
- **No imbalance in the relationship:** consent will not be freely given if there is imbalance in the relationship between the individual and the controller – this will make consent particularly difficult for public authorities and for employers, who should look for an alternative lawful basis.

You can continue to rely on any existing consent that was given in line with the GDPR requirements, and there's no need to seek fresh consent. However, we will need to be confident that our consent requests already met the GDPR standard and that consents are properly documented. We will also need to put in place compliant mechanisms for individuals to withdraw their consent easily.

If existing consents don't meet the GDPR's high standards or are poorly documented, you will need to seek fresh GDPR-compliant consent, identify a different lawful basis for our processing (and ensure continued processing is fair), or stop the processing.

Infringements of the basic principles for processing personal data, **including the conditions for consent**, are subject to the highest tier of administrative fines. This could mean a fine of up to £17 million, or 4% of our total worldwide annual turnover, whichever is higher.

It follows that if for any reason, we cannot offer people a genuine choice over how we use their data, consent will not be the appropriate basis for processing.

4.1 Children's Consent

There are also specific new provisions on children's consent for online services. There are no global rules on children's consent under the GDPR, but there is a specific provision in Article 8 on children's consent for "information society services" (services requested and delivered over the internet). In short, if we offer these types of services directly to children (other than preventive or

counselling services) and we want to rely on consent rather than another lawful basis for your processing, you must get parental consent for children under 16 – although the UK may choose to lower this, to a minimum age of 13. If you choose to rely on children’s consent, you will need to implement age-verification measures, and make “reasonable efforts” to verify parental responsibility for those under the relevant age.

4.2 Proforma Consent Examples

4.2.1 Publishing name & contact details in District & Multiple District Directories

Each year the District Directories and Multiple District Directory are created to publish personal information (name, address, personal email address, generic email address (where applicable), home telephone number, business telephone number, mobile telephone number and club name) of those members who have a designated role as Club (President or Secretary), District Officer, Multiple District Officer, Council Chairman, MD105 Council Officer (Secretary, Treasurer and Sergeant at Arms) or International (International Director and Past International Director).

A proforma consent form is available in the MD web site (<http://lionsclubs.co/MemberArea/?p=252>) entitled ‘Club Member’s Consent Form (Directory)’.

District Secretary should keep signed copies.

4.2.2 Collecting & processing name & contact details of data subjects and/or organisations to advertise future activities/events

A proforma consent form is available in the MD web site (<http://lionsclubs.co/MemberArea/?p=252>) entitled ‘Club Member’s Consent Form (Advertise Event)’.

Club Secretary should keep signed copies.

4.2.3 Collecting & processing name & contact details of ‘friends of club’ keeping them informed with details of activities organised by your Club

A proforma consent form is available in the MD web site (<http://lionsclubs.co/MemberArea/?p=252>) entitled ‘Club Member’s Consent Form (Friends)’.

Club Secretary should keep signed copies.

4.2.4 Distribution of membership/officer information, service programmes, activities & events

There will be occasions when District and Multiple District Officers wish to contact members with details of other activities, events or programmes which require a member's consent.

A proforma consent form is available in the MD web site (<http://lionsclubs.co/MemberArea/?p=252>) entitled 'Club Member's Consent Form (Distribution)'.

District Secretary should keep signed copies.

5 Fund Raising

The current Data Protection Act and forthcoming Data Protection Bill (enactment of EU Data Protection Regulation (GDPR)) set out six principles that should be applied to any collection or processing of personal data:

1. Personal data must be processed lawfully, fairly and transparently.
2. Personal data can only be collected for specified, explicit and legitimate purposes.
3. Personal data must be adequate, relevant and limited to what is necessary for processing.
4. Personal data must be accurate and kept up to date.
5. Personal data must be kept in a form such as the data subject can be identified only as long as is necessary.
6. Personal data must be processed in a manner that ensures its security.

In general, Clubs must have a data subject's consent to process their data. The 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. **Essentially, this requires data subjects' must "opt-in" rather than "opt out"** - the GDPR specifically bans pre-ticked "opt-in" boxes.

However, this definition is only the starting point for the GDPR standard of consent. Several new provisions on consent contain more detailed requirements. In particular, GDPR sets out various conditions for consent, with specific provisions on keeping records of consent, clarity and prominence of consent requests, the right to withdraw consent, and avoiding making consent a condition of a contract.

You are also likely to need consent under ePrivacy laws for most marketing calls or messages, website cookies or other online tracking methods, or to install apps or other software on people's devices. These rules are currently found in the Privacy and Electronic Communications Regulations 2003 (PECR), but there is a proposal for a new updated ePrivacy Regulation to come into

force at the same time as the GDPR. The Regulation has not yet been finalised, so this guidance does not consider these issues further.

Informed Consent

The guidelines reinforce the fact that consent must be informed. As a minimum, the following information must be presented to individuals to obtain valid consent:

1. The identity of the point of contact within the Club.
2. The purpose of each of the processing operations.
3. The type of data which will be collected.
4. The right to withdraw consent.
5. Details of any automated processing, including profiling.
6. The possible risks of data transfer to non-EU countries in the absence of an adequacy principle from the European Commission and appropriate safeguards, where applicable.

With regards to items (1) and (3), in a case where the consent sought is to be relied upon by multiple Clubs, or if the data is to be transferred to or processed by other Clubs who wish to rely on the original consent, these organisations should all be named.

When seeking consent, Clubs should ensure that they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only for lawyers. Clubs cannot use long illegible privacy policies or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form.

A Club must ensure that consent is provided on the basis of information that allows the data subjects to easily identify who the point of contact within the Club who determines the purposes and means of the processing of personal data, and the purposes of the processing for which the personal data are intended is and to understand what they are agreeing to. The Club must clearly describe the purpose for data processing for which consent is requested.

Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. Ensuring that consent is 'informed' is dependent on the purpose being 'specific'. A data subject cannot consent to something if they have not been adequately 'informed'.

Unambiguous Consent

Consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or

declaration. It must be obvious that the data subject has consented to the particular processing. The following will not be acceptable:

1. Pre-ticked tick boxes.
2. Silence or inactivity of the data subject.
3. Including consent as part of general terms and conditions.
4. The use of opt-out boxes.

Withdrawal of Consent

Data subjects have the right to withdraw their consent they have given, at which point the Club must stop processing their personal data. The data subject's ability to withdraw consent should be as easy as it is to give it.

5.1 Example: include this statement in an application form

When sending out an application form for an event which you ask for information from the organisation, you should insert a tick box with the following wording:

- I, **[data subject name]**, hereby grant **[club name]** authority to process my personal data for the purpose of keeping me informed about the date(s) of future **[name of activity/event]** which I may wish to participate in. I am aware that I may withdraw my consent at any time.

6 Subject Access Request

A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.

Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.

For further details, read 'GDPR - Subject Access Request Procedure' and 'GDPR - Subject Access Request Application Form' which can be found at <http://lionsclubs.co/MemberArea/?p=252>

7 Data subject's rights

You need to check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. These rights include:

-
- **Right to information:** You must provide a minimum level of information to data subjects to demonstrate that their personal information is fairly collected and processed.
 - **Right to access:** You must provide data subjects to the following information:
 - A description of personal data we collect and process.
 - Purpose(s) of the processing.
 - Any recipients or group of recipients to whom the personal data is disclosed.
 - **Right to rectification:** The data subject has the right to rectify any inaccuracies in the personal data held about them without undue delay. Inaccurate data includes incomplete data. This right is closely linked to the right of access.
 - **Right to be forgotten:** The data subject can request that information be erased if they withdraw consent or there is an issue with the underlying legality of processing.
 - **Right to restriction of processing:** The right to restriction of processing allows data subjects, under certain specific circumstances, to prevent clubs from conducting specific processing of their data. It means that a club can store the personal information, it cannot process the data unless the individual gives their consent to lift the restriction or the processing is necessary for the establishment of legal claims, to protect the right of another person or in the interests of the wider public.
 - **Right to notification:** It is the Club's duty to ensure that the data subject is notified of specific activities, and that third parties are notified if the data subject exercises any of their rights in a manner that might be relevant to them.
 - **Right to data portability:** Data subjects can request copies of their personal data in a useful electronic format, which they can then submit to another service.
 - **Right to object:** There are rights for data subjects to object to specific types of processing:
 - Direct marketing;
 - Processing based on legitimate interests or performance of a task in the public interest/exercise of official authority; and
 - Processing for research or statistical purposes.
 - **Right to appropriate decision making:** The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

There are obligations to notify data subjects of these rights at an early stage – clearly and separately from other information.

8 Develop operational policies, procedures & processes

- Document the record of personal data processing activities drawn from the data flow audit and gap analysis.
- Where relying on consent, ensure quality of consent meets new requirements.
- Plan how to recognise and handle data access requests and provide responses within a month.
- Secure personal data through appropriate procedural and technical measures.
- Ensure policies and procedures are in place to detect, report and investigate a personal data breach.

9 Web Site(s) & Cookies

Members' will need to consider the following issues when planning a privacy notice:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?

The following documents on the MD105 web site provide guidance:

- GDPR - Web Site Privacy Statement
- GDPR – Privacy Procedure
- GDPR – Privacy Notice

The Privacy and Electronic Communications Regulations (PECR) sits alongside the Data Protection Act. They give people more privacy in relation to electronic communications.

9.1 Privacy & Electronic Communications Regulations (PECR)

There are specific rules on:

-
- Marketing by electronic means, including marketing calls, emails, texts and faxes;
 - The use of cookies or similar technologies that track information about people accessing a website or other electronic service (see <https://ico.org.uk/global/cookies/>);
 - Security of public electronic communications services; and
 - Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (e.g. caller ID and call return), and directory listings.

9.1.1 What's new in PECR

- Content in electronic communications, metadata related to electronic communications and information on users' devices cannot be accessed without consent, unless it is necessary to provide a service/transmit the data or necessary for billing.
- Consent will no longer be required for non-privacy intrusive cookies. The UK regulator already takes this approach, but that was more lenient than his European counterparts. So consumers will no longer be faced with a pop-up if the only cookies on a website are strictly necessary or anonymous analytical cookies.
- Browser settings can be used as consent for cookies. The Commission has rowed back on its preferred approach to where users set their cookie preferences. Rather than requiring every website operator to have its own set of cookie controls, browsers and software which enables electronic communications should enable users to set cookie preferences, but in a more granular way than is currently possible.
- The Regulation will apply to 'over the top' providers (for example, Facebook Messenger, Skype, Gmail, iMessage, Viber and WhatsApp).
- The Regulation takes into account the Internet of Things as it also ensures the privacy of machine-to-machine communications.

9.1.2 How does PECR fit in with GDPR

PECR is a separate piece of legislation to the GDPR but there are various parallels between the two:

- It is a Regulation not a Directive to increase harmonisation.
- There are huge fines, at the same levels as in the GDPR.
- The same regulator will be used in the UK - the Information Commissioner's Office.
- Extra-territorial effect - non-EU companies providing electronic communications services to EU citizens will be subject to the Regulation.

- It is born from the need to increase transparency for consumers.
- Includes specific reference to use of standardised icons to allow users to quickly and easily understand uses of their data.
- Same definition of consent (and all definitions in the GDPR govern the proposed Regulation).
- Aim of adoption by May 2018 so that there is a simultaneous comprehensive overhaul of the legal framework for privacy and data protection.

10 Member awareness e-learning courses

You may consider computer based GDPR awareness courses:

- <https://www.melearning.co.uk/product-category/gdpr/>
- <https://www.itgovernance.co.uk/shop/product/gdpr-staff-awareness-e-learning-course>
- <https://www.gdprorb.co.uk>

10.1 Video 'What is Privacy?'

<https://www.privacyinternational.org/video/1625/video-what-privacy>

10.2 Video 'What is Data Protection?'

<https://www.privacyinternational.org/video/1623/video-what-data-protection>

10.3 Video 'What is Meta Data?'

<https://www.privacyinternational.org/video/1621/video-what-metadata>

11 Useful links

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr> (UK Information Commissioner)

<http://www.eugdpr.org> (a resource to educate the public about the main elements of the General Data Protection Regulation (GDPR))

<http://enisa.europa.eu> (European Agency for Network & Information Security)

<http://www.itgovernance.com> (IT Governance Network)