Retention, Storage, Sharing and Security of Personal Information

In Lions we collect, hold and process "personal data" as defined in UK data protection legislation. This can be names, addresses, email addresses, an attendance list (at meetings or events) – these are just some examples of the sort of personal data held by Clubs, Districts, or Multiple District.

Compliance with the legislation forms two parts:

a) Specific documentation. This is paying the ICO fee and having appropriately worded Privacy Notices, be it on the website, held by the Club, or on the footer of emails or forms.
b) Looking at the systems utilised, and considering how long we need to hold the information for; where we hold it; how we store the information, and the general security of the data and systems.

In other articles I have already provided information about paying the ICO fee, I continue to draft Privacy Notices for Clubs and Districts, so this article is about b) above.

Data Retention

Just how long do we need to hold data for? The law on this point is particularly vague, there are no set retention periods in data protection laws, but there is a reason for this! It is to allow each organisation, in the case of UK Lions, each part of the organisation (Club, District, MD) to hold different pieces of data for separate time periods.

Some examples of this within a Lions Club;

Financial Information – each club keeps accounts, for the Admin Account and/or Charity Account. UK tax law states that the information supporting the accounts (invoices etc) must be held for six years plus the current year. – A set retention period for this set of data.

Membership Data – Contact information on each member and the meeting minutes are just two examples of this type of data. Much of this information forms the historical record of the club, so in this case, probably an indefinite time retention period.

Friends of Lions / Volunteers / People Served – Some of this information may be held for the historical record of the club, but some may become outdated, so the retention period may change and some can be 'weeded out'.

The general rule is to hold data for the period of time that you need it! But as you can see from what I have said above, this can be different for different types of data.

Data Storage

This means 'how we hold data'. So, simply put, this needs to be secure!

On Paper – There is no need to hold all records electronically. If paper records work best for your club, then that's fine! The officers should show the data respect by keeping paper records in, for example, a lockable drawer or in a lockable filing cabinet. Another member of the household or the Lions Club / District Cabinet should be aware of where the data is held. This means that the data can

be passed to an ''appropriate person', should the Lion holder of the data become incapacitated in some way. (see also security further down)

Electronically – There is no requirement to install expensive encryption software to protect data, BUT, you can implement systems for secure storage of personal data held.

a) File it! This may seem straight forward, but you can save an email and / or any attachments in a folder away from the inbox. This will make it easier to find the information when you want it!
b) Backups – Make a backup of the data you hold. This can be stored on disk, USB flash drive, external hard drive or in the cloud (One Drive or Drop Box for example) – all inexpensive methods of data storage that are available to Clubs.

Sharing Data

We need to share data within the Club / District / MD or between different parts of the organisation. Indeed, when we enter a new members details onto MyLCI and obtain an LCI membership number, we are actually sharing the data with LCI.

Data needs to be shared when the mantle of an officer's position passes from one member of the Club to another at the end of the Lionistic year.

If we are to get away from being the 'Best Kept Secret', we must share data – i.e. letting the world know what we do and how we do it! – This can be on social media, especially Facebook. This is 'sharing data'!

There is nothing in the law that prevents us from doing this, and nor should there be!

There are a couple of 'rules' to bear in mind when sharing data –

a) Does everybody in the world need to see this information? – Can you justify sharing it?
b) How have I phrased the information?
c) Would I accept information about me phrased in that way? – remember that any personal information 'recorded' (electronically or on paper) can potentially be accessed by the person it refers to!

Data Security

So, retention, storage and sharing of data do NOT mean that security of data has gone out of the window! Indeed, earlier I said that someone else in the household / Lions Club / District Cabinet should know where the data is held, should the unexpected occur. For electronic data, this could be 'where will I find the passwords?' – It could be sharing a file with this information in it with someone you trust, just remember to update it when passwords change.

It could mean setting up cloud based storage, where only Club Officers can access data in certain files. Access should be restricted to those who need it – This is data security.

Computers / Laptops / Mobile Phones should be password protected.

Websites

Many websites have an SSL certificate. This is shown by a padlock on the left side of the website address bar at the top of the browser. This shows that reasonable security measures are in place on the website and the data it holds.

If you have information in a pdf file for example, there is free software available to download that can password protect these files.

Website members areas can be password protected.

To sum up – keep data behind a form of barrier – where that barrier can be opened by an appropriate person, as and when required.

Paper Records – Just keep them out of general view – perhaps a lockable drawer.

A final note – There is no requirement to go overboard with security measures.