Data Protection Compliance with Lynx

Revision 1.0

March 2018

Overview

The European General Data Protection Regulations are set to change in May 2018. This guide shows you how you can remain compliant with the law after that date.

In general, the new law will mean among other things that:

i) You must have a legitimate reason for any 'Personal' data you hold about a living individual ('Data subject'). This can include names, addresses, telephone numbers and Email addresses, as well as general correspondence. It will generally apply to all Lynx Lead, Customer and Contact records as well as associated attachments, notes and similar items which might be connected via quote and project records.

ii) The Data Subject (typically your customer) must be told the purposes for which you intend to capture and use information about them. This is something you should cover off in your general Terms and Conditions, making it plain what information will be kept, and why. You can keep data for which you have a 'legitimate interest' (such as to provide information in a quote, or to progress a job) without obtaining consent from the data subject provided it does not compromise their interests. Anything else, however, requires that you obtain consent, and that consent needs to be informed, explicit and active (you can't rely on 'small print' in a contract clause, or an opt-out box.

iii) Where you do have consent, you should record how and when it was obtained.

iv) Using the information you hold on leads or customers for marketing, without consent, is most definitely not allowed

v) Once information is no longer relevant for the purposes for which it was recorded, you must remove it

Lynx has several features which make it easier to remain compliant with Data Protection legislation. You should use these and actively manage your data protection compliance to avoid potential breaches of the law.

Capturing Consent for Marketing and Data Retention

When you enter details of a Lead or Customer in Lynx, one of the options you have is to set the flags which allow you to block marketing communications. By default, these blocks will be turned on. If you turn any of them off, Lynx will prompt you to give details of how and when consent was obtained to send marketing communications. The source of consent will be a 'soft' list in the Lynx System Configuration. The details of the consent will be logged in a note (which cannot be deleted) as well as in the consent field on the lead record. This is important as it allows you to provide evidence of compliance in the future.

Note that once you are on the version of Lynx with the new GDPR features, the block flags will be switched on for all Lead and Customer records automatically, enabling you to start capturing consent going forward.

Automated Removal of Lead Information

In general, the main potential source of concern within Lynx is information you hold about Leads. Information about Customers which is not used to actively market them is something you are entitled to hold because you have the legitimate interest of being able to provide service in the future – for example guarantee works or beyond that assistance with repairs.

Lead information, however, needs to be actively discarded after it ceases to be reasonable to hold it. You should therefore have a policy for how long you will retain lead information, after which is must be removed. A reasonable period of time is perhaps 6 or even 12 months, as it is not uncommon for people to take this long to obtain planning consent, funding or come to a decision.

The new GDPR tools in Lynx use a configuration field in the System, Configuration (DELETE_LEAD_AFTER_DAYS) which defaults to 9999 (days). You will need to set this to a more reasonable value, perhaps 180 days, when you are ready to implement the GDPR changes and cull your Lead database.

There is an automatic process 'System Cleanup' on the Lynx Admin menu which can be run as required or configured to run daily and which will mark as 'DEAD' all leads created before this time ('cut-off date'), under the following circumstances:

i) The Lead has not been converted to a customer
ii) There have been no notes, to-do items, quotes, emails, attachments or projects created or actioned on the lead or any associated quote or project since the cut-off date.
iii) The lead name, email or telephone fields are not all blank
iv) The 'Retain Until' field on the Lead has not been set (in which case the Retain Until date will be act as the cut-off date)

On the first run of the System Cleanup, after setting the number of days to keep in the system configuration, you may well find that there are thousands of records to delete.

The process will also delete any Lead records which are already marked dead and which have a creation date 30 days or more before the cut-off date. In other words, you have 30 days grace to restore the record **Note that this may not apply to leads marked deleted in the first run if their creation date is more than a month before your cutoff date**).

When a Lead is deleted in this way, all associated notes, to-do items, attachments, Emails, quotes and projects will also be deleted. In the case of quotes and projects, their associated notes, to-do items emails and attachments will also be removed.

Overriding Lead Deletion

As indicated above, you can keep a lead active by adding data such as a note or Email message. You can also set the 'Retain Until' field. When setting the latter you will be asked to add a commentary for why you wish to retain the record, which enables you to document the reason. As with changes to the blocks on marketing, changes to this date will be logged in a note which cannot be deleted.

Why are customer records not deleted?

You will always have a legitimate reason for retaining customer data, i.e. performance of contract or retaining the ability to provide after-sales service. These interests will never in practice be detrimental to the interests of the customer (Data subject) therefore deletion is not required unless the customer asks you to do so after your contractual obligations and potential obligations under guarantee have ended.

It is recommended under these (likely very rare) circumstances that you amend name, telephone and Email address information to indicate that it has been removed at the request of the customer, and also remove any file attachments that contain personal data. You should also note the fact that this has been done at their request. You can also use this technique to remove Lead data in the

unlikely event that you are asked for removal by the Data Subject prior to the normal housekeeping process taking effect.

What else should I be doing now?

As mentioned above, you should be looking to re-draft your standard terms and conditions so that the information you will retain for your legitimate interests and the ways in which Data Subjects can obtain a copy and request deletion.

If you want to market to existing customers in the future, you should also be contacting them now to get them to opt in. This means they have to give you a positive 'yes' to receiving marketing materials by whatever means. For new customers, consider something like an opt-in box on your satisfaction questionnaire, if you use one.

Staff awareness is also important, and you will need to make your team aware of the changes to the law and how it affects them and your company processes, as well as becoming familiar with the legislation changes yourself.