GDPR for AXLR8 Commercial Clients

1 Introduction

General Data Protection Regulations (GDPR) come into force on 25th May 2018.

They will replace the existing Data Protection Act which has evolved and been amended since 1974 in the UK. Fines for breaking the rules are 4% of turnover or EUR20,000,000 (twenty million Euros) whichever is the lower. There are broadly two groups of responsible people for GDPR. The Data Controller (DC) and where you outsource the data handling to someone else, the Data Processor (DP - probably AXLR8 and others if you are reading this document). Under DPA, the data controller carried most of the responsibility. Under GDPR, the responsibilities of the DC and DP are defined according to their respective functions.

2 Implications for businesses.

1. Care of private data
2. New rights for citizens

2.1 Protection and Security of personal data

It will be a very costly affair if you lose private data and this means you need to maintain procedures for confidentiality amongst your staff and within your office. Regardless of where you data is held, and regardless of whether it is staff data, supplier or customer contacts, you may be penalised if you lose it, expose it or even if, through no fault of yours, it is stolen, compromised or made public when you promised to store it safely. If it becomes used for any reason other than those for which you asked the permission of the subjects, you will also be at financial risk.

So, the key action is to list your data assets and make sure they are securely locked away in the same way as you would your own possessions or any possession you had agreed to hold for a third party.

This permission element leads us on to the second duty we have as Data Controllers.

2.2 Permissions and Citizens rights

The individuals whose data you hold now have very strong rights because of the danger that information theft can have for citizens. For example, a town or date of birth may seem harmless if exposed. However, these items can be used to aid identity theft and fraud if used in combination. As another simple example, holiday tickets contain data than can help a burglary.

2.3 Permissions

The regulations state that we must ask for permission, as businesses to hold data and state the reasons why we need to hold it and for how long.

2.3.1 Opt In

So, if you collect information for direct mail, you need to obtain the citizen's permission. This must be an active Opt In. This differs from the present "unsubscribe" link at the bottom of all AXLR8 newsletters.

The individual MUST OPT IN if you are going to send them email after 25th May 2018.

AXLR8 have created a special field for this. (Previously, we only had the "Send HTML Mailshots" lookup which would have a value of "no" if they unsubscribed). The Opt In field may be inserted into a number of media so your prospects and clients have ample opportunity to do so.

Practical Actions before 25th May 2018

1. Ask you clients in as many ways as possible now to Opt In and record the decision for audit trail with a date stamp in your system.
2. Send out at least one Newsletter to you staff, Members, clients, prospects and other groups encouraging them to Opt In.
3. Add Opt In to your contracts so that staff and suppliers and customers and other groups know they cannot do business with you without certain types of commercial communication. Reasonable material might include:
    a. Invoices
    b. Pay slips
    c. Payment advice
    d. New terms and changes to existing terms
    e. Product news of importance
    f. Product recalls
    g. Product options
    h. Service alerts

However, it would be unreasonable to add to your contractual terms that people who have ceased doing business with you must accept unsolicited advertising direct mail third party recommendations or sharing of their data unless there is some special agreement in return for an incentive such as a service provided free at the point of delivery that is accepted as paid for by those adverts.

2.4 Citizen rights

1. The right to subject access requests: As with DPA, there is a right for the individual to see what data you hold about them.

2. The right to be forgotten: this means, if the individual wishes to be taken off your data base, you have no right to refuse unless you can prove it contravenes some other regulation (e.g. HMRC statutory payroll history you need to keep for 6 years) or they have, for some valid reason, agreed. The later might be where they have ordered goods but have not yet paid.
3. The right to rectification: The individual may ask you to correct

NB All the above rights include any media, files, databases, backups, and most worryingly, all the "shadow IT" of spreadsheets and files that individuals in your organisation may have extracted over the years or created in order to perform analyses or processing.

You must therefore maintain an asset register of all your data systems and you must either prevent people extracting or storing spreadsheets and other data bases, pictures, CCTV, etc of individuals or have a sign out sign in and destruction control procedure – just like a physical asset.

Practical Actions before 25th May 2018

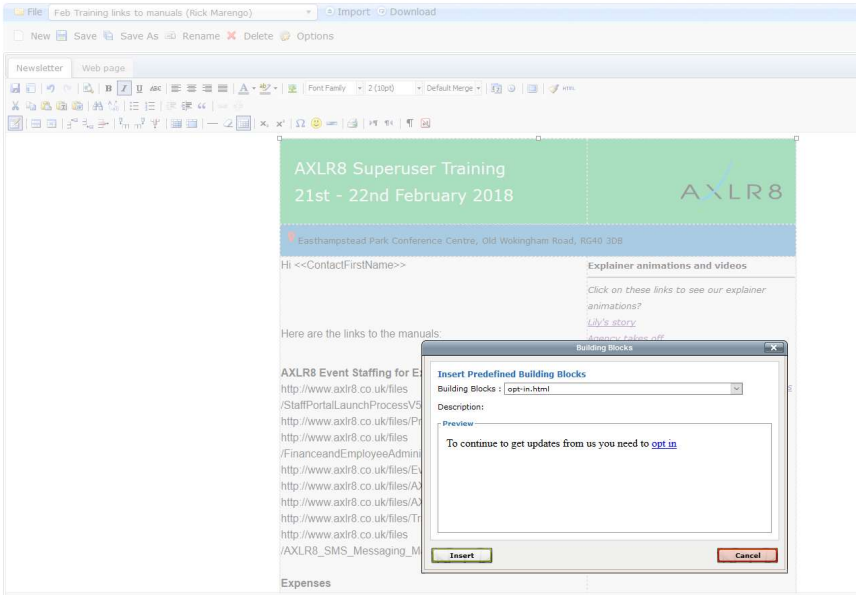
1. user training for AXLR8 Clients
2. Please make sure you switch off "Export to CSV" across your organisation.
3. Change your contracts to agree reasonable terms under which you may collect and retain people's information in certain circumstances. Explain carefully:
    a. Why you need it (e.g. their address so you can collect their laundry or their cell number for 2FA)
    b. How long you will need to keep it (e.g. staff details for payroll for 6 years)
    c. What circumstances they can change/ delete
    d. Who and how they contact your organisation to do so.
4. Make sure that there is a solid disciplined process in place (in the unlikely event you do not have one already) for assuring no adverse information such as notes or ratings are added to staff or client/member/prospect/supplier records.
5. Delete any information you do not need and put in place regular reviews to remove private data. This is especially the case with the ubiquitous spreadsheets that are present in every organisation with private data on them.
6. Define which devices are in scope. Do you supply smart phones? Do these have address books with client data synchronised with your central systems? What happens when people's personal (BYOD) devices are used in the business and they are also synching data. What happens when those people leave. How would you enforce return/ destruction of the data they hold?
7. Make sure that the people responsible for the citizens rights to deletion and rectification are not just trained in GDPR but also have understood how to operate your AXLR8 CRM for cleaning up data. This is covered in the following link:
   AXLR8 data Cleaning
   This document explains how to delete and correct private and other information about individuals.
   http://www.axlr8.co.uk/files/AXLR8DataCleaning.pdf

How the AXLR8 Opt In works

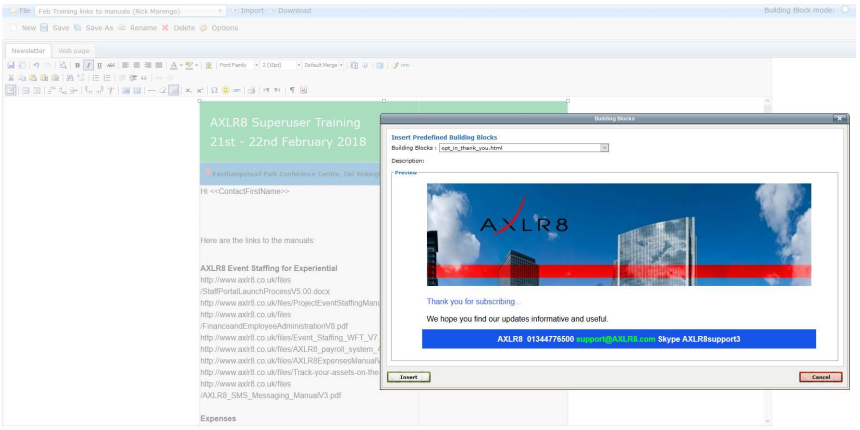
The Opt In is a link that is created wherever you want in your newsletter or other email template. Add the Opt In URL in as many places as you can in as many places in the Newsletter as you wish. Perhaps:

- behind a clear hypertext link in bold
- on a picture of a newspaper and a cup of coffee
- in your email signatures

And don't forget to ask people on the telephone, when y meet with them and in supplier and staffing contracts. Change the opt in link Building Block as you wish. Create as many BBs as you wish. The Opt In link is secure and so needs to be configured for each client. This is happening in and orderly queued basis through March - April 2018



Once you have added the Opt In BB, you can also edit the "Opt In Thank you" BB and change that to add your own branding. This is the page they go to when they have Opted In
If they skip the Opt In, clearly there is no page to go to.
They can still always go to the unsubscribe link.



Feel free to ask our designers to help if you do not have in-house designers.