helpful

Helpful client site GDPR review

The General Data Protection Regulation (GDPR) brings data protection legislation into line with new ways that personal data is now used. For website owners, it's an opportunity to tidy up the way we manage user data with transparent privacy practices in mind. It's also a legal obligation by 25 May 2018 with steep penalties for non-compliance.

Personal data under the GDPR includes "any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier". For instance, names, email addresses or identifiable IP addresses all constitute personal data.

GDPR checklist for data controllers from the ICO
12 steps to take now to prepare for the GDPR (PDF)

You should ensure that within your organisation you:

1. are registered with the ICO as a data controller/processor
2. have documented the personal information you hold
3. have documented on what basis you are processing user data (what data, why processed, where it is kept, who has access to it, how long it is retained for) - usually as part of a data protection policy
4. have ensured you have taken sensible steps within your organisation to keep information secure, and put a process in place to report breaches of security to the ICO – usually as part of an information security policy and breach notification policy
5. have ensured the contracts you have with processors of your data include explicit roles and responsibilities for data controllers and processors?
6. have considered how to ensure the information you hold is current, accurate and up to date
7. have gathered and recorded consent for contacts on email lists or site member registrations assembled previously. Consider emailing the contacts again explicitly to check
8. have a retention policy e.g. a point at which data can be deleted when no longer required

Hosting	1. Is the installation well-maintained e.g. software up to date, security plugins active? 2. Are there any pages/posts that shouldn’t be indexed or picked up by spiders? Is robots.txt working correctly?	
Analytics and third party services	3. Which services processing user data are active on the site? Briefly document the data being processed. (e.g. MailChimp, Google Analytics etc) 4. Does the privacy/cookies page report cookies set (for GA or other tools) correctly? Check/document who manages GA profile for the site and ensure all is OK. 5. Does any part of the site pass any personal data e.g. email addresses to Google Analytics e.g. in URL queries? Are user IPs anonymised? (if using GA Dashboard plugin)	
Publishers	6. Are all publishers (especially Administrators) still active and required? If not, remove or demote former users to Subscribers. 7. Do publishers have suitable strong passwords set? (Enforce with security plugin)	
Newsletters	8. Does the site collect user details for newsletter list or other subscriptions, and if so is clear consent obtained and recorded at the time? 9. Do newsletters have a clear method to opt out/unsubscribe? 10. Which tool is used to hold subscriber data, and is it covered by EU/US privacy agreements? 11. Are there any old/test lists stored in the tool which should be removed?	

Forms	12. Are forms used on the site to collect user data and is consent clearly obtained for this processing? 13. Is data from form submissions retained for only as long as required for processing? (e.g. not just building up in Gravity Forms entries. Clear out/disable saving of form data as entries where it is not needed) 14. Are there any integrations with 3rd parties leading to data and information being stored in multiple places?	
Members areas	15. Does the site have an area which users can log in to? If so, are login cookies documented and is content obtained when the user registers for this area? 16. What information is requested from users? Is there a clear rationale explained to users for what is collected and does it seem reasonable?	
Privacy policy	17. Does the site have a clearly-linked privacy policy which contains all the key information (incl correct cookies), including how data is processed when submitted through other channels e.g. complaints, job applications, social media enquiries, FOI requests etc? 18. Does the privacy policy include clear contact details to handle questions or subject access requests?	
Social media & plugins processing user data	19. What plugins, if any, are active which send user data to be processed by a third party? 20. Are social media plugins active on the site which track user activity? If so, are their cookies identified and/or their privacy policies referenced from the main policy?	

Subject access requests	22. How can a user request a machine-readable copy of their submitted data? 23. How can a user request erasure or correction of their data?	
Offline data	24. Is any data (test or live) stored offline, and if so, is it still required or can it be deleted? 25. Does Helpful hold any client customer data on our own systems (e.g. Dropbox) and if so can this be deleted?	