DIRECT ONLINE MARKETING'S CHECKLIST FOR GDPR COMPLIANCE

1. Analytics
    1. Review and accept the Google Analytics (GA) updated data processing amendment – Here's how:
        1. Analytics -> admin -> account -> account settings -> review amendment — once you have reviewed the amendment, *click done*. Click done again to save account settings.
        2. Make sure your GA tag fires only after you have the user's permission using an overlay cookie acceptance box (be sure that it also contains a link to your terms and conditions). Once you gain user consent, trigger a page reload that fires the GA tag or use a virtual pageview to trigger the GA tag.
        3. More on virtual page views
    2. Check analytics implementation for PII. You can't delete old info but can stop processing by:
        1. Checking existing URLs for PII
        2. Ensuring you don't submit PII upon form submit
        3. Are you using the GA user-ID feature? Admin -> property -> user-ID —- should be alphanumeric if you are using and should not contain any PII
        4. I don't think the length of time needs to be changed but here is where it can be changed from if you desire: analytics -> admin -> property -> tracking info -> data retention
2. Anonymize IPs
    1. Based on using GTM
    2. GTM -> workspace -> analytics tag -> more settings -> fields to set — field name: anonymizeIp, value:true
        1. If using GA snippet:

2. Add this code: ga('set', 'anonymizeIp', true);

3. Privacy Policy updates your team should make:
    1. Contact information for the Data Controller
    2. User rights and how to apply them
    3. How you collect their personal data
    4. How they can choose what types of information you process about them
    5. How you will use their PD
    6. With whom you will share their PD
    7. The names of entities with whom you share their PD for direct marketing purposes
    8. How you secure their information
    9. The legal basis and purposes for processing their PD
    10. The length of time you store their PD
    11. Whether their information will be transferred to other countries
    12. Their right to request, access, change, restrict, make portable, or erase their personal information
4. EU Specific- DPO (Data Protection Officer)
    1. Form a GDPR compliance team
        1. Perform a GDPR readiness (compliance) assessment
            1. Assign a Data Protection Officer
                1. *Note*: The following consists of generalized recommendations. Laws for compliance vary by jurisdiction, and you should check with local laws regarding how to comply in your area.
                2. You need a DPO if:
                    1. You are a public authority (except for courts acting in their judicial capacity);
                    2. Your core activities require large scale, regular and systematic monitoring of

individuals (for example, online behavior tracking); *or*

3. your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offenses.

3. Checklists for compliance
    1. Appointment of a DPO
        1. You are a public authority, are required to appoint a DPO, and have appointed a DPO (except if you are a court acting in your judicial capacity – in which case you are not required to appoint a DPO).
        2. You are not a public authority, but you know whether the nature of your processing activities requires the appointment of a DPO.
        3. You have appointed a DPO based on their qualifications and knowledge of data protection law and practices within the EU.
        4. You aren't required to appoint a DPO under the GDPR but you have decided to do so voluntarily. You understand that the same duties and responsibilities apply had you been required to appoint a DPO. You support your DPO to the same standards.
    2. Position of the DPO

    1. Your DPO is given independence to perform their tasks and reports only to your highest level of management.
    2. Your DPO must be informed promptly of all matters related to data protection.
    3. You must ensure your DPO has the necessary resources required to perform his duties.
    4. You cannot in any manner penalize the DPO for performing their duties.
    5. Any tasks assigned to your DPO outside of their position cannot contain any conflict of interest.
3. Tasks of the DPO
    1. The DPO is tasked with monitoring your compliance with GDPR and providing relevant policies, awareness-raising, training, and audits.
    2. Your DPO is promptly informed with any data compliance issues and is included in the solution.
    3. In the UK, your DPO is required to be the contact point for the ICO.
4. Accessibility of the DPO
    1. Your DPO is easily accessible as a point of contact for all employees and has an open line of communication with the ICO.

        2. You must publish the contact details of the DPO and relay them to the ICO.
    2. Implement policies and procedures for how to respond to data subject' rights requests
    3. Create a written record of current processing activities and work-flow for personal data
        1. Document your legal basis for each processing activity
    4. Update your privacy and security policies
    5. Write and publish protocols for what to do in the case of a data breach
        1. Time frame of notification?
        2. How to notify?
        3. Who to notify?
5. Email Lists
    1. Consider:
        1. Run an opt-in campaign (aka permission passing campaign) for email list subscribers. This is to qualify leads and validate demand for your email messages, ensuring maximum deliverability and engagement, while decreasing rejection
            1. We recommend that you run an email campaign with at least three emails that gives users a change to opt-in following changes to GDPR regulations. End with email – "Last chance to Opt-in"
        2. Unify all existing email databases
        3. Exclude all contacts who have previously opted out
        4. Create a segment in all email and marketing databases (or automation software) for EU / UK demographic
        5. We recommend you launch a sequence
6. Working with third parties

1. Purchasing/ renting email lists – if you sent/scripted the email, you are on the hook w/o legal protection
    1. Only work with vendors that guarantee their lists only contain contacts who have opted into receiving relevant communications.
    2. Even if you have taken the necessary steps to ensure your vendor is compliant and have a liability clause in your contract with the vendor that removes you of blame, you could still end up with the following if the contacts are not GDPR compliant:
        1. GRPD violation from EU authorities
        2. A lawsuit with the third party (initiated by you) to sue for damages
2. Email delivery vendor
    1. Removes you of the liability
7. Inbound lead information collection compliance
    1. Web forms on your site (or that you control elsewhere)
        1. Do not use pre-checked boxes on forms
        2. Don't have to worry about ANY other steps if you turn double opt-in in
        3. Refer to compliance recommendations according to your form builder's site:
            1. MailChimp – About the General Data Protection Regulation
            2. New MailChimp Tools to Help with the GDPR