[GDPR for Online Business] - Roadmap to Compliance - Review and Checklist

Business Name:_____

Data Completed:_____

Name of Person Completing:_____

Email Address:_____

Complete This Checklist and Email the Completed Roadmap to flor@mccarthy.ie for your Free Roadmap Review

Item to Consider	Record Your Situation	Decision / Action
Does GDPR apply to you territorially? It does if you process the personal data of EU residents otherwise than on an occasional basis no matter where you are based.		Yes/No Action required: When:
Do you process personal data? If you process data that is capable of identifying a living individual resident in the EU wholly or partly through automated means or as part of a physical filing system you process data. Processing includes collection, use and storage.		Yes/No Action required: When:

Do you process special categories of personal data? Data revealing racial or ethnic origin, political opinions, religious racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation.		Yes/No. Action required: When:
Do you process data relating to criminal convictions?		Yes/No Action required: When:
Do you process the personal data of children? A child for the purposes of the GDPR as a person under the age of 18 years. The age at which a child may provide consent consent for services provided for payment at a distance by electronic means – e.g. paid online service may be 13. Individual member states may specify older ages for consent.		Yes/No Action required: When:
Does your business have an establishment in the EU? If your business is not established in the EU and you process personal data of EU residents		Yes/No Action required:

otherwise than on any occasional basis (or any basis if special categories of data or criminal convictions) you are obliged pursuant to Article 27 of the GDPR to designate in writing a representative in the EU. The representative must be established in one of the Member States where the data subjects are and must be mandated by you to be addressed in addition to or instead of you by the Data Protection authority in that Member State on all issues relating to processing of data.		When:
What level of turnover in your business involves the personal data of EU residents?		Level:
Can you segment your list to identify with certainty which parts of it involve the personal data of EU residents?		Yes/No Action required: When:
If your business does not have an establishment in the EU and you process data of EU residents, have you appointed an Article 27 Representative?		Yes/No Action required: When:
What are my lawful grounds for each of the processing activities that I have identified? • the data subject has given consent to the processing of his or her personal data for one or more specific purposes;		Decision

• processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; • processing is necessary for compliance with a legal obligation to which the controller is subject; • processing is necessary in order to protect the vital interests of the data subject or of another natural person; • processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; • processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. • Processing is required for the purposes of providing and obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings. • Processing is otherwise required for the purposes of establishing, exercising or defending legal rights. Where you choose legitimate interest as your ground for processing in particular, you should ensure that you have documented your consideration of this ground and the basis for your decision in choosing it, balancing the risk and rights of data subjects.		Action required: When:

Have you carried out a data inventory? A data inventory is an ongoing record of all categories of data that you hold identified by reference to the various categories of data subject on behalf of whom you hold the data. It is essential to prepare and inventory and keep it update in order to guide you on what you need to do to comply with GDPR on an going basis.		Yes/No Action required: When:
Do you need to appoint a Data Protection Officer (DPO)? A DPO is required where either • your core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or • Your core activities consist of processing on a large scale of special categories of data and data relating to criminal convictions.		Yes/No Action required: When:
If you need to appoint a DPO have you done so? The DPO: Shall be designated on the basis of professional qualifications and, in particular, expert knowledge of data protection law and practices		Yes/No Action required: When:

Supported and provided with resources for their tasks Cannot be dismissed for performing their tasks or given instruction in relation to their tasks Shall report directly to the highest management		
If you have appointed a DPO have you informed the relevant Data Protection Authority?		Yes/No Action required: When:
Have you identified all transfers to third parties and where those third parties are located? Data transferred to third parties should be governed by an appropriate agreement to ensure that data protection principles are complied with and whether there is a transfer outside of the EU appropriate measure must be in place to ensure that this is lawful.		Yes/No Action required: When:
Have you identified whether transfers of data involves transfer to data processors or to other data controllers or joint data controllers? Transfers for purely administrative purposes to third parties who solely process the data on your behalf can be governed by data processing agreements. Transfers of data for commercial purposes, providing others with access to data to use if for their own independent commercial		Yes/No Action required: When:

purposes involves different considerations and will need to be reviewed in more detail based on your circumstances.		
Do you have a GDPR compliant Privacy Notice? Any pre-existing privacy notices that you have are unlikely to be compliant with GDPR and will need to be updated. This includes online notices on your website etc. and other notices to be given to all data subjects under GDPR.		Yes/No Action required: When:
Have you updated your Privacy Notice on your website? You should already have a link to your privacy notice on your website. If not you should add one. You should update your existing privacy notice to a GDPR compliant notice.		Yes/No Action required: When:
Have you sent your updated Privacy Notice to your existing clients, former client and prospects? GDPR requires that all data subjects on behalf of whom you hold data are entitled to be given notice of various things which should be included in your GDPR compliant privacy notice. A copy of this notice should be sent to all data subjects.		Yes/No Action required: When:

Have you added an Opt-In wording to all subscription channels on your website etc.? If you have forms on your website that enable visitors to contact you and subscribe for information and email, you should ensure that the sign up process is GDPR compliant with appropriate wording and a link to your privacy notice.		Yes/No Action required: When:
Have you obtained GDPR consent for marketing communications? Consent for GDPR purposes must adhere to very specific criteria and therefore consent procured before GDPR measure were put in place is unlikely to be compliant. You should consider whether you need to obtain fresh GDPR consent from your existing subscribers. Where you chose a lawful basis for processing other than consent, such as legitimate interest, you should ensure that you have documented the consideration of this ground and the basis for your decision in choosing it, balance the risks and rights of data subjects.		Yes/No Action required: When:
Have you established your lawful basis for processing special categories of data or data relating to criminal convictions? If consent is relied upon for processing special categories of data (such as health and medical		Yes/No Action required: When:

records) or data relating to criminal convictions explicit consent is required. Where processing is justified on the grounds of providing and obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings or is otherwise required for the purposes of establishing, exercising or defending legal rights, then this should be clearly documented and the data used only for this purpose.		
If consent is to be relied upon as the basis for processing special categories of data or data relating to criminal conviction, have you put procedures in place for obtaining and recording explicit consent?		Yes/No Action required: When:
If consent is to be relied upon in relation to data relating to children, have you put procedures in place for obtaining and recording consent?		Yes/No Action required: When:
Have you put in place a system for managing opt-outs/withdrawal of consent? GDPR requires you to keep records of opt-outs. You should ensure that your email marketing systems manages this for you and that you have an audit trail so that you can demonstrate compliance if called on to do so.		Yes/No Action required: When:

Have you put in place GDPR compliant Data Processing Agreements with all third parties to whom you transfer data/ GDPR requires that you must have an agreement in place with all third parties to whom you transfer data (e.g. IT supplier, outsourced payroll, transcriptions, consultants, cloud based services etc.) Where there is a transfer of data outside of the EU further measures must be in place before that transfer can lawfully take place.		Yes/No Action required: When:
Have you put in place a system for recording and responding to data subject access requests? All subject access requests must be recorded and responded to within one month unless there are grounds to extend this period based on the complexity and volume involved.		Yes/No Action required: When:
Have you put in place a system for recording data breaches, determining whether notification is required and making notification? All data breaches must be recorded and notified to the Commission within 72 hours of becoming aware of them unless the breach is unlikely to result is a risk to rights and freedoms of natural persons. All data breaches likely to result in a high risk to the rights and freedoms of natural persons must be notified to the data subject.		Yes/No Action required: When:

Do you have comprehensive Data Protection Policies in place? Your Data Protection Policies should include: Retention/Deletion Policy Data Security Policy Breach Handling and Notification Policy Access Request Policy Accuracy policy Right to be forgotten policy Data portability policy		Yes/No Action required: When:
Do you need to carry out a Data Protection Impact Assessment (DPIA)? A DPIA is required when the processing is likely to result in a high risk to the rights and freedoms of natural persons.		Yes/No Action required: When:
Do you engage in automated individual decision making or profiling? If you engage in automated individual decision making or profiling, the data subject has the right to be informed of this and not to be subject to it,		

except in certain circumstances, most notably that the subject has given explicit consent.		
If consent is to be relied upon as the basis for automated individual decision making or profiling, have you put procedures in place for obtaining and recording explicit consent?		Yes/No Action required: When:
Have your reviewed your security? You need to review your arrangements to ensure the physical security of the data that you hold (both on your premises and when taken off site) and your cyber security for all data that you hold in electronic form.		Yes/No Action required: When:
Have you reviewed your insurance, is it adequate? It is strongly advisable to have appropriate insurance to cover the risks you face as a data controller and that you review any insurance now to ensure that it is adequate in light of the additional obligations and risks arising as a result of GDPR.		Yes/No Action required: When:

If you have employees who are EU residents, have you established your lawful basis for processing data you hold on behalf of employees and have you provided your employees with the notices that they are entitled to? Consent arrangements or otherwise in previous contracts of employment are unlikely to be sufficient consent for GDPR purposes and therefore, you need to establish your lawful basis for continuing to process employee data and you need to provide your employees with the notices that they are entitled to as data subjects.		Yes/No Action required: When:
If you have employees, you have arranged data protection training for them? Everyone on your team needs to understand their role in data protection and their responsibility in dealing with data on behalf of data subjects. All employees should know what to do to keep data secure and to prevent breaches. All employees should know what to do if a data subject access request is received, if a data breach occurs or if the firm receives a complaint or is contacted by the Data Protection Commission. Ongoing training and internal meetings need to be held on a regular basis and documented. This is your responsibility to ensure that you team knows what they need to know.		Yes/No Action required: When:

Complete This Checklist and Email the Completed Roadmap to flor@mccarthy.ie for your Free Roadmap Review