# Brokers Ireland Guidance on Direct Marketing

# Data Protection and E-Privacy

July 2020

*This document and information contained within is intended by Brokers Ireland as an aid to Members, to assist in their meeting their obligations under the Act. It is not intended to be relied upon as constituting legal advice to Members on how they are to discharge their professional obligations. Should Members have queries relating to their professional obligations and how these might be discharged, specific legal advice should be taken*

Brokers Ireland
87 Merrion Square, Dublin 2, D02 DR40.
t: 01 661 3067
e: info@brokersireland.ie
www.brokersireland.ie

BROKERS IRELAND

# CONTENTS

## THE REGULATORY ENVIRONMENT

In addition to the GDPR and the Data Protection Act, there are rules which specifically apply to electronic direct marketing (marketing conducted by phone, fax, text message, and email) which are set out in the The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. 336 of 2011), "the ePrivacy Regulations".

If sending electronic direct marketing, then the legislation that applies in the first instance is the e-Privacy Regulations. The ePrivacy Regulations are to be read together with the rules found in the Data Protection Act 2018 and GDPR.

Additionally, Brokers will also be aware of the Consumer Protection Code and what is required when contacting consumers (Chapter 3.40 - 3.45). Even though not specifically aimed at direct marketing, the Code should be considered, please see the attached link:

https://www.centralbank.ie/docs/default-source/regulation/consumer-protection/other-codes-of-conduct/unofficial-consolidation-of-the-consumer-protection-code.pdf?sfvrsn=7

The GDPR governs the processing of the personal data of an individual, while ePrivacy laws refers to **any information** being processed/used for the purposes of unsolicited marketing to customers via electronic means, not just personal data.

Postal marketing is not subject to ePrivacy laws, nor is marketing that is solicited (directly asked for) by the customer.

## LEGAL BASIS FOR PROCESSING

Each data processing activity that you carry out requires a legal basis (under GDPR) such as consent or legitimate interest[1].

However, if sending direct **electronic marketing** then the legislation that applies in the first interest is ePrivacy Regulations. Under ePrivacy Regulations you can only process data using consent as the lawful basis (except in very limited circumstances).

The European Data Protection Board issued Opinion 5/2019: where the ePrivacy Directive (and by extension the ePrivacy Regulations) requires "consent" to be obtained, the controller cannot rely on other lawful grounds provided under GDPR. According to the EDPB only consent may be relied on as the legal basis for processing, and it is not possible to rely on legitimate interests or any other legal basis for processing. There are very limited circumstances where consent is not required, and as a legal basis must be present to process the data, then legitimate interest may be used. See *Marketing Channels, Pt 3 Email (Existing Customers – Individuals and Businesses) Page 11.*

Where consent is required from the data subject to send direct marketing to their device or their phone, or so called soft option consent in the context of a sale, then you cannot use any other lawful basis under GDPR as the e-Privacy Regulations takes precedence and will apply in the 1st instance.

This does not apply to direct marketing using the postal service, as this does not fall within the definition of "electronic mail" in the e-Privacy Regulations, and therefore the legal basis of legitimate interest may be used.

[1] The other four lawful basis are in short; 1) it is necessary for the performance of a contract, 2) it is necessary for compliance with a legal obligation, 3) it is in the public interest and 4) to protect the vital interests of the data subject.

It should be noted that silence, pre-ticked boxes, or inactivity on the part of the data subject will not constitute consent under GDPR, and therefore will not be sufficient to demonstrate consent for the purposes of direct marketing, where required, under either GDPR or the ePrivacy Regulations.

**Exception to rule that consent is required**

Regardless of your GDPR legal basis, **under ePrivacy legislation**, consent is not specifically required in respect of every instance of electronic direct marketing, and there is an exception to the general requirement for consent, but only in cases involving existing customers and when sending the communication by email, fax or SMS/text, where **all of the following are met**:

(i) At the point of sale, the personal data was collected in the context of the sale,

(ii) The product or service being marketed is your own product or service;

(iii) The product or service you are marketing is of a kind similar to that which you sold to the customer at the time you obtained their contact details;

(iv) At the time you collected the details, you gave the customer the opportunity to object, in an easy manner and without charge, to their use for marketing purposes;

(v) Each time you send a marketing message, you give the customer the right to object to receipt of further messages; and

(vi) The sale of the product or service occurred not more than twelve months prior to the sending of the electronic marketing communication or, where applicable, the contact details were used for the sending of an electronic marketing communication in that twelve-month period.

The GDPR further requires that the customer's electronic mail contact details (email address, fax number, number for texts) must have been lawfully obtained in accordance with the Data Protection Act 2018. This means the initial reason for obtaining the contact details must have been compliant with the principles of data protection and have had a valid legal basis, as appropriate for the context in which the electronic mail contact details were originally obtained. As consent is not present, as per above exceptions, you must have another valid legal basis for processing the data i.e. legitimate interest.

In all other cases, consent is required.

## CONSENT

Consent (under the GDPR) must be: freely given, specific, informed and unambiguous (obtained through a clear, affirmative action). Pre-ticked boxes, opt-outs, silence or inactivity do not indicate valid consent.

Consent should be able to be withdrawn as easily as it is given.

***Consent should be:***

**Unbundled**

- Consent should be kept separate from other terms and conditions and should not be a pre-condition of signing up for a service;

**Granular**

- Consent should be collected for each distinct processing operation or marketing channel. Examples of "processing operations" could be consumer behaviour analysis, profiling, segmentation of an email list, combining data from third parties. Ideally, you should provide a check-box for each one;

**Named**

- Your organisation and any third-party who will be relying on the consent should be named (precisely defined categories of third-were parties will not be enough);

**Kept under review**

Once you have gained consent you must keep it under review. People have only given consent for the specific processing they told about when the data was collected. If your organisation wishes to change any of the processing activity, or use the data for another purpose, you must inform the individual and obtain further consent.

**As easy to withdraw as give it**

Organisations must tell the individual that they have the right to object to further marketing, and this right should be notified to them at each instance a marketing communication has been issued to them, and they have the right to withdraw consent at any time also. They should be able to withdraw it as easily as they gave it.

**An organisation must give an individual the following information for consent to be considered specific and informed:**

**The Purposes of the processing**

Why does your organisation need this personal data? Make your reasons for requesting it very clear. Individuals need to be informed about all the types of processing being undertaken.

**Change in the processing of the data**

If data processing which the individual was not informed about takes place, consent will not be informed, so it will not be considered valid.

**Organisations should also consider the following when processing data:**

**Duration**

How long consent lasts will depend upon the individual context, so organisations should determine the duration themselves. The organisations should also document this retention period and why they chose it in their records of processing activities. For products such as insurance which renew annually, it might be appropriate for consent to last a year.

**Audit Trail**

Keep an audit trail of those who consented, when they consented, what they were told at the time, how they consented and if consent has been withdrawn, include date, time and method of withdrawal.

Sample Consent statements are included in the Appendices A - D

## LEGITIMATE INTERESTS

**The legal basis of legitimate interest can only be used in respect of marketing communications issued by post, or in respect of the very limited circumstances where consent is not required when marketing by email/fax/text – See page 11 for more information.**

Article 6 of the GDPR says that '*Processing will be lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or 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.'*

What this means is that firms must weigh up their right as a business to market to someone against their right to privacy. Firms must offer a clear opt-out and have a compelling case for why someone may be interested in their goods or services. Put very simply legitimate interests means that if the processing of personal data is a fundamental part of your day-to-day business, without which you would not be able to function, then you should be allowed to continue to do so.

If you determine that legitimate interests is the most appropriate legal basis for your data processing, you must be able to show that you have balanced the interests of the business against the rights and freedoms of the individual.

If you have an existing relationship with the customer and believe your marketing activity would be reasonably expected by them and have provided an opportunity to opt-out at the point of data collection and at every subsequent communication, then legitimate interests may be considered as an option for your legal basis for processing.

In determining if your marketing activities would be "reasonably expected", consider factors such as how long ago you collected the data and where you sourced it. Think about the nature of your existing relationship and how you have used the individual's data in the past. Are you using a new technology or processing data in a new way that they may not anticipate?

To determine if legitimate interests is the correct legal basis for your processing activities, you must carry out a Legitimate Interests Assessment (LIA). A template for this assessment is included – Appendix F

**The Legitimate Interests Assessment (LIA) has three parts:**

1. **Identify your Legitimate Interest**
   For marketing, this is usually "communicating with customers or prospects to help promote or sell products or services"

2. **Necessity Test**
   You must demonstrate that all the processing activities you carry out, are completely necessary to achieve your purpose. For example, sharing personal data with a third party that they do not need to carry out a service on your behalf would be considered unnecessary. E.g., using a postal mailing company but including the customers phone number in the data you send them. If there is another reasonable and less intrusive way to achieve the same result, you should not rely on legitimate interests. You may have more than one purpose for processing personal data, for example, sending a marketing communication and segmenting an email list into different customer groups. You need a legal basis for each of these and they could be different.

3. **Balancing Test**
   In this part of the test, you balance your interests against the rights and freedoms of the individual. If a person would not expect you to use their data in that way or it would cause them harm, it is likely that legitimate interests is not the correct legal basis for your processing. You should identify any risks in this section and also outline safeguards you have put in place, for example, promising to delete data after a certain time period or only requesting the minimum, essential personal data you need to carry out your campaign.

Upon completion of the Legitimate Interests Assessment (LIA) you will need to reach a decision as to whether Legitimate Interests is the most appropriate legal basis. Record your thinking and document your decision to show you have proper decision-making practices in place.

Your choice to use consent or legitimate interests for direct marketing has an impact on the rights of the data subject. The right to erasure of their data is automatic if you are relying on consent. If relying on legitimate interest, the company has the opportunity to justify the legitimacy of the processing before having to erase data. If you are relying on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects. The right of data portability does not apply if relying on legitimate interest, it only applies when relying on consent or contractual necessity.

## NEXT STEPS

| Task | Notes |
|---|---|
| Identify and list the data sets (or groups of people) you send marketing communications | Clients, event attendees, website signups, sub-contractors etc |
| For each data set, list the types of personal data collected and the purpose for collecting each | Name, email address, phone number etc |
| For each data set, list the methods used to collect the data | In-person (paper sheets), website, phone call, bought-in lists etc |
| For each data set, list the channels for marketing communications | Email, phone, post etc |
| List all third parties who process any part of the data on your behalf | Email systems like Mailchimp or any other marketing tools where personal data is uploaded/stored. |

When you have all this information, you will need to decide whether **consent** or **legitimate interest** is the most appropriate basis for marketing to each data set.

| If consent | If legitimate interest |
|---|---|
| Examine the nature of the consent already gathered and establish if this is GDPR or E-Privacy compliant. Was it explicitly received? Was it clear and unambiguous? | Conduct a Legitimate Interests Assessment and document results (this legal basis can only be used in very limited circumstances; refer page 4) |
| If not, plan a solution to re-attain consent. | If using legitimate interest, as a legal basis, update the privacy notice/statement to reflect this and implement additional safeguards.<br><br>If not in favour of retaining legitimate interest, plan a campaign to move to consent. |

In parallel with the actions above, you will need to continue with planning GDPR compliant processes for data to be collected in the future, including:

- Ensuring consent remains valid and up to date
- Updating Privacy Policy
- Updating Privacy Notice/Statement
- Where using third-parties, ensure you have a data processing agreement in place.

## MARKETING CHANNELS

1. **Post**
2. **Telephone**
3. **SMS/Text messages**
4. **Email (existing customers – individuals and businesses)**
5. **Email (non-customers – individuals and businesses)**

### 1. Post

As advised earlier, the ePrivacy Regulations do not apply to direct marketing to postal addresses, as this form of marketing does not fall within the definition of "electronic mail" in those regulations. However, the requirements of GDPR and the Data Protection Act still apply and must be met where the marketing is addressed to a particular individual as opposed to "owner/occupier".

You must obtain consent from your customers (or potential customers) to use their data for marketing purposes and advise them at point of collection that they may withdraw such consent at any time. The consent must be given freely and explicitly. (Opt-in). It must be specific, informed and unambiguous. They should be able to withdraw their consent as easily as they gave it. A firm cannot send unsolicited marketing mail if the address was originally collected for an entirely different purpose. Firms must not send marketing mail to anyone who objects or opts out from such marketing. Firms must comply with any objections or opt-outs promptly.

For non-customers, you can use names and addresses on the most up-to-date version of the Edited Electoral Register but not the Full Register for postal marketing. Individuals on the Edited Register are those who, when registering to vote, did not object to personal data being used for marketing.

Local authorities publish two versions of the Register of Electors – the full register and the edited register (also known as the open register). The edited register is an extract of the electoral register but is not used for elections. It can be bought by any person, company or organisation. The **Edited Register** contains the names and addresses of voters who have given their permission for their details to be used for other purposes (for example, for direct marketing use by a commercial company or other organisation).

It is an offence for an organisation to use the full electoral register for direct marketing purposes. Find out more about how to deal with unsolicited direct marketing material.

**ALL OF THE FOLLOWING marketing channels are subject to e-Privacy rules**

### 2. Telephone

In relation to telephone calls, the ePrivacy Regulations do not distinguish between unsolicited telephone communications to individuals and those to companies (and all other persons other than natural persons). How they are regulated depends on whether they are calls to landlines, or to mobile phones.

**Landlines:** Unsolicited marketing calls to landline phones are permitted unless and until the intended recipient notifies the firm conducting the marketing, that they do not consent to receipt of such a call. (Opt-out basis).

**Mobiles:** Unsolicited marketing calls to mobile phones are prohibited unless the firm undertaking the marketing has been notified by that individual that they consent to the receipt of those calls on the mobile phone (that is, an express opt-in is required).

An exception exists where the person has recorded their consent to direct marketing calls on the National Directory Database.

In respect of both landline and mobile contact, in the case of a customer, you can call them if they have previously given you consent, even if they have opted out from receiving marketing calls on the National Directory Database ("NDD"), i.e. the consent given to your firm outweighs the preferences recorded on the NDD and so you do not need to check the NDD. However, in the case of a non-customer, you must check the NDD for any opt-outs recorded before calling that individual, i.e. the NDD opt-out will override any consent given to your firm.

Further information please see
https://www.comreg.ie/consumer-information/home-phone/unsolicited-contacts-national-directory-database-2/
https://www.comreg.ie/consumer-information/mobile-phone/unsolicited-contacts-national-directory-database-2/

NDD and FAQ'shttps://www.dataprotection.ie/en/organisations/rules-electronic-and- direct-marketing/ndd-faqs

Direct marketing companies and Brokers would be required to purchase a copy of the NDD to see which phone numbers do not want to receive 'cold calls' and make sure that they do not call them. However, it can take up to 28 days after the information is recorded in the NDD for marketers to access the opt-out listing. This depends on how often they update their own listings.

### 3. Email (existing customers – individuals and businesses)

When sending direct marketing messages by electronic mail existing customers, the general rule is that consent must be obtained from the person to whom the marketing communication is to be addressed. (The consent should satisfy the GDPR standard). At the point of sale, you must obtain consent for the purpose of marketing, and provide your customers with an opportunity to object to (or opt-out) of the use of their details for electronic direct marketing at any time going forward.

For those existing customers who do not opt-out, i.e. they do not object to the use of their details for electronic direct marketing, you can email them for marketing purposes, as long as **all of the following criteria are met**:-

(i) At the point of sale, the personal data was collected in the context of the sale;
(ii) The product or service being marketed is your own product or service;
(iii) The product or service you are marketing is of a kind similar to that which you sold to the customer at the time you obtained their contact details;
(iv) At the time you collected the details, you gave the customer the opportunity to object, in an easy manner and without charge, to their use for marketing purposes;
(v) Each time you send a marketing message, you give the customer the right to object to receipt of further messages; and
(vi) The sale of the product or service occurred not more than twelve months prior to the sending of the electronic marketing communication or, where applicable, the contact details were used for the sending of an electronic marketing communication in that twelve-month period.

This is the only exception to the general rule that consent must be obtained.

**4. Email – Non-customers (individuals and businesses)**

For non-customers that are individuals you must have their prior explicit consent (i.e. opt-in) before emailing them for marketing purposes.

However, non-customers that are businesses you can email them for marketing purposes as long as their business or official email is received by you in the context of commercial or official activity or is listed in a Business Directory. However, you must ensure there is legitimate interest, as you must have a lawful basis for processing the data.

Electronic mail communications to businesses for the purpose of direct marketing are permitted unless and until the intended recipient notifies the firm that they do not consent to receiving such communications (that is, the marketing can take place on an opt-out basis) (regulation 13(4), ePrivacy Regulations).

It should be noted opt-outs, silence, pre-ticked boxes, etc. will not satisfy the requirements for consent defined under GDPR, and therefore will not demonstrate consent for the purposes of electronic marketing where required under e-Privacy Regulations.

In all cases, a person sending an electronic mail for the purposes of direct marketing must include a valid address at which the sender may be contacted (regulation 13(10)(c), ePrivacy Regulations).

All direct marketing by electronic mail must also comply with the GDPR and the Data Protection Act 2018.

**5. SMS/Text messages**

SMS/Text messages are considered like email and the same rules apply.

## All direct marketing campaigns

As stated earlier, GDPR and the Data Protection Act 2018 also apply to direct marketing. As a form of processing of personal data, any direct marketing activities must comply with the GDPR generally. This includes compliance with the key principles set out in Article 5, including:

- Fair and lawful processing
- Collected for specified, legitimate purpose
- Retained for no longer than is necessary
- Data minimisation.
- Accuracy of all data processed for direct marketing purposes.

Among other generally applicable obligations, the GDPR also requires a controller of personal data for direct marketing purposes to provide certain information about its processing activities (that is, by way of data protection notice), including the intended purposes for the processing of the personal data (i.e., direct marketing).

It must also not be forgotten that where data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data for marketing purposes. The right to object must be communicated to the data subject in a clear manner. They also have the right to withdraw consent at any time, and this should be communicated to the data subject before consent is given. They should be able to withdraw consent as easily as they gave it.

## SPECIAL CATEGORIES OF DATA

The GDPR defines certain types of personal data as *"Special Category"* data. This includes:

> ***"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"***

If you wish to use any of this data in your marketing, you must obtain explicit consent from the individual in the majority of cases and should take extreme care in ensuring this data is not misused or accessed without authorisation.

## THIRD-PARTY VENDORS

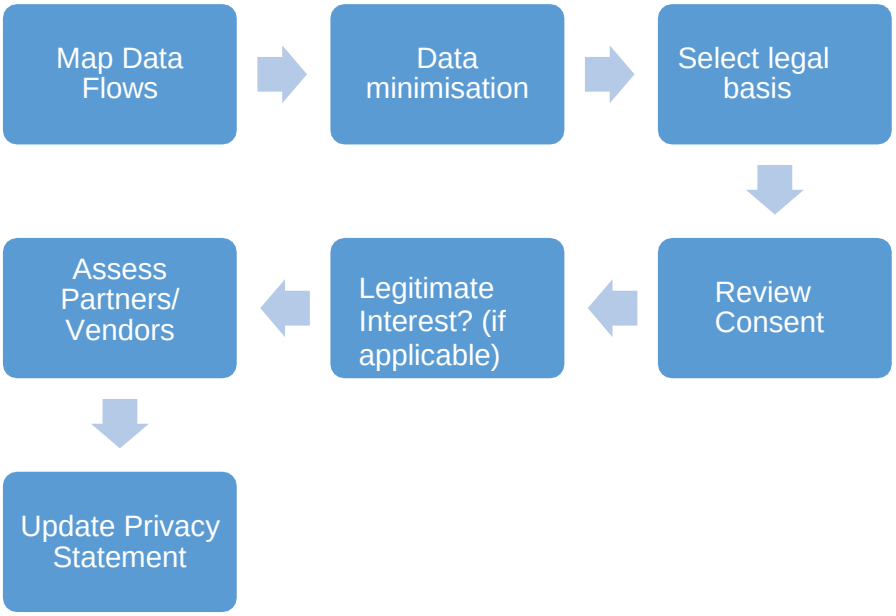
If you use third-party tools or platforms to help with your marketing (email services, postal mail fulfilment, SMS messaging companies etc), pursuant to Article 28(3) of GDPR you will need to have a data processing agreement in place with each one. This agreement ensures that you (the Data Controller) and your service provider (the Data Processor), clearly understand your respective responsibilities and liabilities in processing personal data.

The agreement must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller. Contracts must also include at a minimum, the following terms, requiring the processor to:

1. Only act on the written instructions of the controller;
2. Ensure that people processing the data are subject to a duty of confidentiality;
3. Take appropriate measures to ensure the security of processing;
4. Only engage sub-processors with the prior consent of the controller and under a written contract;
5. Assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
6. Assist the controller in meeting GDPR obligations in relation to security of processing, the notification of personal data breaches and data protection impact assessments;
7. Delete/return all personal data to the controller as requested at the end of the contract
8. Submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing upon the GDPR or other data protection law of the EU or a member state.

## CONCLUSION

**How should companies move towards GDPR compliant marketing?**




1. **Map your Data Flows**

   Think about what data you have, how you gathered it, why you have it, who has access, how you share, store and secure it, how long do you keep it and how do you dispose of it.

2. **Data Minimisation**

   Do you need all of the information that you currently have? Why do you have it? Consider a data clean-up exercise if you have unnecessary data in storage.

3. **Selection of Legal Basis**

   Ask yourself which parts of your direct marketing activities are done on the basis of consent and which use legitimate interests (very limited circumstances).

4. **Review Consent**

   Look at your consent forms across your organisation and revise the language on these, if necessary, to ensure they are GDPR appropriate. Make sure you have good systems in place to store those records of consent and retrieve them quickly in the case of an audit or investigation. Consider if you will need new IT tools to help you with this or automated preference management tools to allow individuals to login in and manage their own communication preferences.

5. **Complete a Legitimate Interest Assessment (LIA)**

   If you must use legitimate interest as your basis for any of your processes (in the limited circumstances where consent is not required), complete the LIA. Document the results and your decision-making process. See page 20 for copy of sample LIA.

6. **Assess Partners and Vendors for GDPR Compliance**

   Ensure you have a data processing agreement in place with your partners and vendors (these would include your IT service providers, outsourced payroll support, CRMs etc). See page 13.

7. **Update Privacy Statement**

   Ensure your privacy statement is GDPR compliant. Make necessary changes so that your clients are fully informed of why you collect their data, how you process and store it, and who you share it with.

## FAQs ABOUT MARKETING UNDER THE GDPR

**1. Can I use Bought-In Lists?**

You can use bought-in lists to make live marketing calls, but you should screen against your own 'do-not-call' list of people who have previously objected to or opted out of your calls.

You must be very careful before using bought-in lists for recorded calls, texts or emails. You can only use them if those on the list specifically consented to receive that type of message from you. Generic consent covering any third party is unlikely to be enough.

You must make checks to satisfy yourself that any list is accurate, the details were collected fairly, the information provision obligations have been met and that the consent is specific and recent enough to cover your marketing.

**2. Can I send unsolicited email to someone if their address is publicly available on their website?**

You will need to consider both the GDPR and ePrivacy in this scenario. Under ePrivacy:

- For non-Business (i.e. individuals) non-customers: You must have their prior explicit consent (i.e. Opt In) before emailing them for marketing purposes.
- However for Business non-customers (even individuals such as sole traders for example) - you can email them for marketing purposes as long as their business or official email is received by you in the context of commercial or official activity or is listed in a Business Directory

**3. Can I send unsolicited marketing by post to someone that is not my customer?**

The ePrivacy Regulations do not apply to sending direct marketing by post. Therefore, it is only GDPR that you need to consider. Under GDPR, as you will generally not have consent initially, you may be able to rely on legitimate interests to send a first mail but you must try to obtain consent to continue sending further communications.

The basis of legitimate interests is not a blanket solution to sending direct marketing by post to huge lists of addresses scraped from the internet. This is a violation of the GDPR. You must be able to justify why you chose a specific person in an organisation to send marketing to and you should be able to show that you adhered to the GDPR principles of legality, fairness and transparency in the process used to obtain their address. To be able to rely on legitimate interests, you need to be able to show that you have a strong reason to contact the individual, and the organization. Both of your organisations are likely to benefit from a potential business relationship, you have informed them you are processing their data and given them a clear way to opt-out of further communications. You must also keep in mind the principle of only storing data for as long as needed. If you do not receive a response to your mailing, remove the data from your list in a timely manner.

**4. Can I Share Lists with other companies in the group?**

If you intend to share the list within your group and you have chosen consent as your legal basis, then you must have the individual's specific consent to receive marketing material from the group of companies.

If legitimate interests is your chosen legal basis for this processing, you must carry out a Legitimate Interests Assessment (LIA). You should consider why they want the information, whether they actually need it, and what they will do with it. You need to demonstrate that the disclosure is justified, but it will be the receiver's responsibility to determine their lawful basis for their own processing.

# APPENDICES

## A. Sample Consent Form 1

Here at [**Company Name**] we take your data protection seriously and will only process your data as advised to you in our privacy statement. *State here how clients can access your privacy statement…*

However, from time to time we may wish to contact you in relation to… *insert here why you will be contacting your customers e.g. new products, updates etc***.**

**Agreed Methods of Contact:** (Tick all that apply)

- ☐ Email
- ☐ Phone
- ☐ SMS
- ☐ Post
- ☐ Fax
- ☐ Please do not contact me

Even if you do subscribe now you can always unsubscribe at any time.

## B. Sample Consent Form 2

*(Basic form, for companies with simple marketing communications)*

We would love to send you special offers, information on products you may like and news about [**Insert Company Name**] by email, phone, post, SMS or other electronic means.

We will treat your personal data with respect and never sell your details to third-parties for marketing purposes. We will only process your data as advised to you in our privacy statement. *State here how clients can access your privacy statement…*

(Tick all that apply)

- ☐ Yes please, I'd like to hear about special offers and product information
- ☐ No thanks, please do not contact me with special offers and product information

Even if you subscribe now, you can always unsubscribe at any time.

## C. Sample Consent Form 3

*(Form for companies who are part of a group or larger entity where other parts of the organisation may use the gathered customer data. It can be used for companies who match the data they gather with data from external services to form a bigger profile of the customer)*

We would love to send you special offers, information on products you may like and news about [**Insert Company** Name] by email, phone, post, SMS or other electronic means.

We will treat your personal data with respect and never sell your details to third-parties for marketing purposes. We will only process your data as advised to you in our privacy statement. *State here how clients can access your privacy statement…*

Would you like to receive information from [**Insert Company Name**] and partners? (Tick all that apply)

- ☐ I would like to receive information from **[Insert Company Name]**
- ☐ I would like to receive information from **[Insert Name of Partner]**

In addition to the data you provide, we may match this with data from third-party profiling services to better personalise our communications with you and recommend products you may like. (Tick if applicable)

- ☐ Allow matching with third-party services

Even if you subscribe now, you can always unsubscribe at any time.

## D. Sample Consent Form 4

*(Lots of detail, allows the customer very granular control of their data. Useful for companies who do a lot of segmenting and personalisation and generally use a third-party email marketing tool to manage this)*

From time to time [**Insert Company Name**] has news about our products and services that we hope you'd like to hear about. Tell us know how you would like us to communicate with you (Tick all that apply).

- ☐ Email
- ☐ Phone
- ☐ SMS
- ☐ Post
- ☐ Fax

How often would you like to hear from us?

- ☐ Weekly
- ☐ Monthly
- ☐ Quarterly

What would you like to hear about?

- ☐ Tips and guides to help you get the most from the products you have purchased from us
- ☐ News about our Company or Industry
- ☐ Details of New Products and Services
- ☐ Special Offers
- ☐ Requests for your Feedback

We will never sell your data and we will keep it safe and secure.

If you would prefer not to hear from us, you can stop receiving our updates at any time by getting in touch with us at [**Insert contact details**] or by clicking the unsubscribe link at the bottom of our emails.

For further details on how your data is processed and stored, click here (this link will lead to your privacy statement).

## E. Detailed Customer Communication Policy

[**Company Name**] would love you to be among the first to hear about special offers and news about our products and services. We communicate with you in various ways including email, postal mail, Phone, Fax and SMS *(Delete accordingly).* We will make sure our contact with you is relevant based on the information you give us.

We will never pass your personal information to anyone outside of our company for them to use for their own marketing purposes.

Your privacy is our priority, so we will always make sure you are in control of everything we do with your personal information.

Here is a list of the items we may wish to contact you about:

- Tips and guides to help you get the most from the products you have purchased from us;
- News about our company or industry;
- Details of new products and services;
- Special offers;
- Requests for your feedback.

You can opt-out at any time by contacting us at *[insert email],* by calling us on *[insert phone]* or by clicking the 'Unsubscribe' link at the bottom of any email you have received from us.

We will always comply with Irish and European data protection legislation and you can see how we do this by reading our full privacy policy here *[insert link].*

## F. Sample Legitimate Interests Assessment Template (LIA)

| Part 1: Purpose Test |
|---|
| **You need to assess whether there is a legitimate interest behind the processing:** |
| 1. Why do you want to process the data? |
| 2. What benefit do you expect to get from the processing? |
| 3. Do any third parties benefit from the processing? |
| 4. Are there any wider public benefits to the processing? |
| 5. How important are the benefits that you have identified? |
| 6. What would the impact be if you couldn't go ahead with the processing? |
| 7. Are you complying with any specific data protection rules that apply to your processing (e.g. profiling requirements, or e-privacy legislation)? |
| 8. Are you complying with other relevant laws? |
| 9. Are you complying with industry guidelines or codes of practice? |
| ***Are there any other ethical issues with the processing?*** |
| Part 2: Necessity Test |
| **You need to assess whether the processing is necessary for the purpose you have identified:** |
| 1. Will this processing actually help you to achieve your purpose? |
| 2. Is the processing proportionate to that purpose? |
| 3. How can you achieve the same purpose without the processing? |
| ***Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?*** |
| Part 3: Balancing Test |
| 1. You need to consider the impact on individuals' interests rights and freedoms and assess whether this overrides your legitimate interests. |
| 2. A first step here would be to evaluate your data processing. If upon evaluation, you believe are risks within your processing, you should consider carrying out a Data Processing Impact Assessment (DPIA) to further analyse these risks. |
| Nature of the Personal Data |
| Is it special category data? |
| Is it data which people are likely to consider particularly 'private'? |
| Are you processing children's data or data relating to other vulnerable people? |
| Is the data about people in their personal or professional capacity? |

| Reasonable Expectations |
|---|
| 1. Do you have an existing relationship with the individual? |
| 2. What's the nature of the relationship and how have you used data in the past? |
| 3. Did you collect the data directly from the individual? What did you tell them at the time? |
| 4. If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? |
| 5. How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? |
| 6. Is your intended purpose and method widely understood? |
| 7. Are you intending to do anything new or innovative? |
| 8. Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation? |
| ***Are there any other factors under these circumstances, that mean they would or would not expect the processing?*** |
| Likely Impact |
| 1. What are the possible impacts of the processing on people? |
| 2. Will individuals lose any control over the use of their personal data? |
| 3. What is the likelihood and severity of any potential impact? |
| 4. Are some people likely to object to the processing or find it intrusive? |
| 5. Would you be happy to explain the processing to individuals? |
| 6. Can you adopt any safeguards to minimise the impact? |
| ***Can you offer individuals an opt-out? Yes/No*** |
| Making the Decision |
| This is where you use your answers to Parts 1, 2 and 3 to decide whether you can apply the Legitimate Interests Basis. |
| 1. Can you rely on legitimate interests for this processing? Yes / No |
| 2. Do you have any comments to justify your answer? (optional) |
| ***LIA completed by:***<br><br>***Date:*** |
| Next Steps |
| Keep a record of the Legitimate Interests Assessment (LIA)<br>Review it at regular intervals<br>Do a Data Processing Impact Assessment (DPIA), if necessary.<br><br>***Include details of your business purposes and lawful basis for processing in your privacy notice, including an outline of your legitimate interests.*** |