

PRIVACY POLICY

1. What does this Privacy Policy cover?

This is our main Privacy Policy and it explains how Data Ireland (“we”, “us” or “Data Ireland”) use Personal Data which we collect about individuals. “Personal Data” is information about living individuals.

We use the words Personal Data to describe any information we hold that is about you or other individuals, and from which you or they are identifiable. Our aim is responsible handling of Personal Data and this Privacy Policy describes how we use Personal Data that we collect as part of our functions. This includes Personal Data obtained from a variety of sources listed in paragraph 3 below.

This Privacy Policy may be supplemented by other privacy notices tailored to specific activities. This is to make sure you have a full picture of how we collect and use your Personal Data.

We accept from you personal data about another individual only if you (a) inform the individual about the content of this Privacy Policy and any other applicable privacy notices provided to you; (b) obtain their permission to share their Personal Data with us in accordance with this Privacy Policy and other applicable privacy notices; and (c) obtain any legally required consent, where applicable.

2. Personal Data we hold

The Personal Data we hold about you and other individuals differs depending on our relationship, including the type of communications between us and the services we provide. Personal Data we may hold and process includes:

- **Contact information**
- **Marketing preferences, marketing activities and customer feedback**
- **Lifestyle data, age category, place of residence, family composition, household income, car ownership and/or hobbies / interests**
- **Profiling**

3. Sources of Personal Data

3.1 We may obtain Personal Data from the following sources:

- (a) our websites at www.dataireland.ie and www.business.ie (the “Websites”); and
- (b) email;
- (c) telephone surveys and calls, directly or through third parties working on our behalf to update our databases;
- (d) from businesses in respect of individual contact details within such businesses; and
- (e) data brokers who have obtained your consent to use your personal data for third party marketing purposes.

4. How we use Personal Data

We use Personal Data to carry out our business activities, further details of which are available on our Websites. The purposes for which we use your Personal Data may differ based on the services we provide. These include our ownership and operation of the Irish Consumer Marketing Database and business contact details on www.business.ie.

The main purposes include using Personal Data to:

- 4.1 enable us and our clients to undertake advertising, marketing, direct marketing and public relation exercises;
- 4.2 provide a full range of database management services to our clients, including supplying consumer and business data, data profiling, data hygiene, data capture and address validation and correction;
- 4.3 perform accounting and other record-keeping functions;
- 4.4 provide personnel, payroll and pension administration services; and
- 4.5 supply identity verification for use in anti-fraud and anti-money laundering processes.

5. Responsibility for Personal Data

Data Ireland is responsible for looking after your Personal Data in accordance with this Privacy Policy, our internal standards and procedures, and the requirements of data protection law.

When we provide Personal Data to third parties providing services to us or engage a third party to collect Personal Data on our behalf, the third party service providers (data processors) will be selected carefully and required to use appropriate measures to protect the confidentiality and security of the Personal Data. Those third parties will assume certain responsibilities under data protection law for looking after the Personal Data that they receive from us.

6. Sharing of Personal Data

In connection with the purposes described above, we may need to share your Personal Data with third parties (this may involve third parties disclosing Personal Data to us and us disclosing Personal Data to them). These third parties may include:

Type of third party	Examples
Clients	Businesses or individuals who wish to use our data for the purpose of sending direct marketing (subject to your preferences) or otherwise contacting you. These may include small and medium enterprises (“SMEs”); manufacturers, financial services providers; government and semi-state bodies; utility companies and retail companies. We also supply other data suppliers and marketing agencies who broker our data to their customers, and these parties are required to comply with data protection and e-privacy laws in the use of the data including observing any marketing preferences expressed.
Our service providers	External third party service providers, such as security professionals, accountants, auditors, experts, lawyers and other professional advisors; travel assistance providers; call centre service providers; IT systems, support and hosting service providers; advertising, marketing and market research, and data analysis service providers; banks and financial institutions that service our accounts; document and records management providers; printing service providers; and other third party vendors and outsourced service providers that assist us in carrying out business activities.
Database providers or publications	For the purpose of providing verification or ‘data hygiene’ services to our clients as set out in sections 4.2 and 4.5 above, we obtain (or have obtained) information from publications (e.g. Stubbs Gazette for verifying company directors) or other public registers and providers of databases and registers such as Demographics Ireland and, up to May 2015, the An Post Redirection Service.

7. **Processing of Personal Data**

For the purposes set out above we may transfer Personal Data to clients and service providers located in other countries.

In the event that we transfer Personal Data to countries outside the EEA that have data protection regimes which are different to those in the EU, , we take steps to ensure that your Personal Data is adequately protected and transferred in accordance with the requirements of applicable data protection law.

This may involve the use of data transfer agreements in the form approved by the European Commission or another mechanism recognised by data protection law as ensuring an adequate level of protection for Personal Data transferred outside the EEA (for example, the standard contractual clauses approved by the European Commission).

For further information about these transfers and to request details of the safeguards in place, please contact us using the details below.

8. **Security of Personal Data**

Data Ireland uses appropriate technical, physical, legal and organisational measures that comply with data protection laws to keep Personal Data secure.

As most of the Personal Data we hold is stored electronically we have implemented appropriate IT security measures to ensure this Personal Data is kept secure. For example, we use anti-virus protection systems, firewalls, and data encryption technologies. We have procedures in place at our premises to keep any hard copy records physically secure. We use electronic access cards with secret PIN to manage access to all areas in our premises. We also train our staff regularly on data protection and information security.

Unfortunately, no data transmission over the Internet or electronic data storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any Personal Data you might have sent to us has been compromised), please immediately notify us.

9. **Legal justification for our use of Personal Data**

To comply with the law, we need to tell you the legal justification we rely on for using your Personal Data for our purposes.

While the law provides several legal justifications, the section describes the main legal justifications that apply to our purposes for using Personal Data:

9.1 Justification for processing Personal Data:

- (a) Where necessary for performing a contract to which you are a party or to take steps at your request prior to entering into this contract;
- (b) Your consent (where you voluntarily give consent to provide us or a third party with your Personal Data); and
- (c) Where necessary for the purpose of our legitimate interests or those of a relevant third party.

9.2 Where we rely on our legitimate business interests or the legitimate interests of a third party to justify the purposes for using your Personal Data, our legitimate interests will usually be:

- (a) pursuit of our commercial activities and objectives, or those of a third party (for example, by carrying out direct marketing or conducting market research);
- (b) compliance with applicable legal and regulatory obligations;

- (c) development of any guidelines, improvement and development of business operations and service offerings;
- (d) conducting analytical and statistical research and profiling.

10. **Monitoring communication**

We monitor electronic communications between us (for example, emails) to protect you, our business and IT infrastructure, and third parties including by:

- (a) identifying and dealing with inappropriate communications; and
- (b) looking for and removing any viruses, or other malware, and resolving any other information security issues.

11. **Retention of Personal Data**

We will keep Personal Data for as long as is necessary for the purposes for which we collect it.

Where we hold Personal Data to comply with a legal or regulatory obligation, we will keep the information for at least as long as is required to comply with that obligation.

Where we hold Personal Data in order to provide a product or service to you as a client, we will keep the information for at least as long as we provide the product or service, and for 7 years thereafter.

In relation to consumer names and addresses these are periodically deleted where they have not been used in a marketing campaign in over 12 months . If you opt out of receiving direct marketing, we will keep a record of this indefinitely in order to ensure that your marketing preferences continue to be observed.

In relation to business contact data, we deactivate the Personal Data after 24 months from the date of its last verification. It is only reactivated following fresh verification and subject to this Policy.

For further information about the period of time for which we retain your Personal Data, please contact us using the details below.

12. **Personal Data Rights**

The following is a summary of the data protection rights available to individuals in the EEA in connection with their Personal Data. These rights may only apply in certain circumstances and are subject to certain legal exemptions.

- Right of access to a copy of your Personal Data;
- Right to withdraw consent to processing of Personal Data (where we process on the basis of consent);
- Right to rectify any Personal Data we hold about you if it is inaccurate or incomplete;
- Right to have your Personal Data erased from our systems in certain circumstances e.g.
 - if your Personal Data has been processed unlawfully;
 - if you object to our processing of Personal Data on grounds relating to your particular situation and we have no overriding grounds to continue to use it (see below); or
 - where you have provided consent to processing and you wish to withdraw the consent.

- Right to restrict (i.e. suspend) our processing of Personal Data (This may be requested while the accuracy of your Personal Data is being established by us in the event we receive a rectification request or while we assess an objection received by you (see below));
- Right to data portability where your Personal Data, which you have provided to Data Ireland with your consent, is processed by automated means;
- Right to object to our processing of your Personal Data on the basis of our legitimate interests (see paragraph 9.2 above) on grounds relating to your particular situation. However, we may continue to use your Personal Data, despite your objection, where there are compelling legitimate grounds to do so or if we need to use your Personal Data in connection with any legal claims or where we have one or more other legal basis to process your Personal Data (see paragraph 9 above);
- Rights relating to automated decision making and profiling having legal or similarly significant effects on you – Data Ireland does not engage in such decision making or profiling on this basis and therefore these rights do not apply.

If you wish to exercise your rights, please contact us using the details below.

You also have a right to complain to the Irish Data Protection Commission if you think that we have processed your Personal Data in a manner that is not in accordance with data protection law. If you are based in another EU Member State, you may complain to your local data protection regulator.

13. **Who to contact about your Personal Data**

If you have any questions or concerns about the way your Personal Data is used by us, you can contact us by e-mail at: datacompliance@dataireland.ie or by writing to the Data Protection Co-Ordinator, Data Ireland, Ground Floor, 89-94 Capel Street, Dublin 1, D01 H0C2.

This Privacy Policy was last updated in May 2018.

We review this Privacy Policy regularly and reserve the right to make changes at any time to take account of changes in our business, legal requirements, and the manner in which we process Personal Data.