

Resolve Ireland Privacy Statement

Introduction

The purpose of this document is to set out the privacy entitlements of Data Subjects, as defined in the General Data Protection Regulation (GDPR), of living persons. Privacy can only apply to information that is not already in the public domain and GDPR only applies to such personal data.

The General Data Protection Regulation (GDPR) is a European Union Regulation that sets out the data entitlements of data subjects and the obligations of those who process the personal data of data subjects. GDPR seeks to protect and enhance the rights of data subjects. These rights cover the safeguarding of personal data, protection against the unlawful processing of personal data and the unrestricted movement of personal data within the EU.

Personal Data

Our company collects data from companies as part of the provision of our consultancy services in a business-to-business context. The consequence is that we may process personal data belonging to the employees of our own company and of our client companies. In this regard we act in the role of data controller, data processor and in some instances as joint controllers with our client companies. We use the data supplied to provide employment related documentation, employment related investigations, disciplinary hearings, management consulting and strategic human resource planning. We do not share any data in our control with any third parties.

We reserve the right to discuss cases internally for such purposes as consultation, training and peer review.

Data Minimisation Principle: We will only collect the information we need so that we can ensure adequate processing of information that is relevant and adequate information and documentation provided to our clients. We do not sell or broker data.

We may process information which includes sensitive or special categories of personal data. We will only process this data when we need to for the purposes of the services we provide, where we are processing the data for a substantial public interest, where we have a legal obligation or where we have consent to do so. Examples of when we use this type of data include:

1. Medical information, for example, where clients or their employees choose to discuss their circumstances with us and this includes medical information.
2. Criminal convictions, we may process this information in the context of compliance with our legal obligations.

Legal basis for processing any personal data

This company relies upon the following legal bases for data collection:

1. Contract: Information is required in order to perform the duties of the consultancy contract between our client companies and ourselves. The basis of data gathering in that instance is contractual requirements. This will include identification information such as but not limited to name, address, email information relating to the creation of a contract and the carrying out of same.
2. Information may be gathered which is sought on the express and explicit consent of the data subjects outside of our contractual and statutory data collection basis.
3. Information is processed in the legitimate interests of the business of our company, and where so processed it will be in accordance with and subject to data subject rights and entitlements.

Consent

Through agreeing to this privacy notice you are consenting to us processing data for the purposes outlined. You can withdraw consent at any time, except where the retention of particular information is necessary for the fulfilment of contractual or legal obligations, by emailing miriam@resolveireland.ie, Data Controller for our company, or by writing to us, see last section for full contact details.

Disclosure

A necessity of our contractual engagement is that we receive and share personal data with our clients in relation to our client businesses. We have in place Data Sharing Agreements or Data Processing Agreements with all such clients relevant to the particular service we are providing our client. We have done our utmost to ensure that all such parties process personal data in a manner that is consistent with this Privacy Notice and GDPR. Our clients may themselves be subject to third party audits either in the form of ethical audits, governmental/statutorily required audits or legal obligations, these are deemed a necessity of the contract of engagement between our client and our company and on this legal basis we may disclose data in relation to our own employees/contractors to be shared to comply with these requirements.

We may disclose Personal Information to meet legal obligations, regulations or valid governmental requests.

We may also enforce our Terms and Conditions, including investigating potential violations of our Terms and Conditions to detect, prevent or mitigate fraud or security or technical issues; or to protect against imminent harm to the rights, property or safety of our company, its clients and/or the wider community.

Retention Policy

We will process personal data during the duration of any contract and will continue to store only the personal data needed for periods after the contract has expired to meet any legal obligations as set out in the table below. After these periods any personal data not needed will be deleted.

Source of Obligation	Retention Period
Contractual obligations with clients	We create a bespoke template for each document pertinent to the needs of our clients. Once the employee information is put through this template and released to the client at the conclusion of an assignment, all such individual documents are updated or destroyed by confidential shredding in-house. All emails are catalogued for client support evidential purposes, but any personal data therein is destroyed once handed over to the client. Any personal data provided in the context of an investigation to which one of our employees or panel members is assigned, is destroyed/deleted as soon as any relevant appeal process following the conclusion of the investigation has expired or as outlined below.
Revenue Commissioners, Collector General, Companies Acts legislative provisions	6 years rolling retention of records
Reports arising from contact through our Protected Disclosure service for client companies	Disclosure Reports and relevant associated documents are retained for 7 years from the date issued to the relevant client
Disciplinary Investigations arising out of client assignments	Investigation Reports are retained for 7 years from the date issued to the relevant client
Culture Audit Reports arising out of client assignments	Culture Audit Reports are retained for 7 years from the date issued to the relevant client.
Grievance Review Reports arising out of client assignments	Review Reports are retained for 7 years from the date issued to the relevant client.
Dignity at Work Investigation Reports arising out of client assignments	Investigation Reports are retained for 7 years from the date issued to the relevant client.
Data Law Compliance	Records in relation to our compliance with Data Law and GDPR will be kept for a five-year period.

Data Breaches

What is a Data Breach?

- Under GDPR, the concept of breach covers more than an unauthorised access, use or disclosure of personal data & includes any breach of security giving rise to accidental or unlawful destruction, loss or alteration of data (which would likely capture data being irreparably corrupted or accidentally wiped, for example), will need to be assessed to determine whether the mandatory breach notification obligations are triggered.

Reporting of Data Breaches

- As per the above it is important to take a broad view of what may constitute a data breach and report all instances immediately to miriam@resolveireland.ie regardless of severity – We will then be able to assess who should be notified.

Responding to GDPR Requests

- If you receive a GDPR request that impacts our service provision, the first step is to confirm the identity of the requestor and then send details to miriam@resolveireland.ie for review.

Data storage

Data is held in Ireland using our own server. We do not store personal data outside the EEA.

Your rights as a data subject

For the entirety of the time that we are in possession of personal data, data subjects have the following rights:

- **Right of access** – you have the right to request a copy of the information that we hold about you.
- **Right of rectification** – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- **Right to be forgotten** – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- **Right to restriction of processing** – where certain conditions apply you have a right to restrict the processing.
- **Right of portability** – you have the right to have the data we hold about you transferred to another organisation.
- **Right to object** – you have the right to object to certain types of processing such as direct marketing.
- **Right to object to automated processing, including profiling** – you also have the right not to be subject to the legal effects of automated processing or profiling.

These rights may on occasion need to be modified/curtailed by statutory or competing obligations, for example, you may request that we delete your data. In the event that we are obliged to refuse your request in accordance with your data subject rights, or if we are obliged to place conditions on our assent to your request, we will provide you with a reason as to why,

which you have the right to legally challenge. At any time following a request from you we can confirm what information we hold about you, as well as how and why it is being processed.

request the following information:

- Identity and the contact details of the person or organisation that has determined how and why to process your data.
- Contact details of the data protection officer, where applicable.
- The purpose of the processing as well as the legal basis for processing.
- If the processing is based on the legitimate interests of our company or a third party such as one of its clients, information about those interests.
- The categories of personal data collected, stored and processed.
- Recipient(s) or categories of recipients that the data is/will be disclosed to.
- How long the data will be stored.
- Details of your rights to correct, erase, restrict or object to such processing.
- Information about your right to withdraw consent at any time.
- How to lodge a complaint with the supervisory authority (Data Protection Regulator).
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether you are obliged to provide the personal data and the possible consequences of failing to provide such data.
- The source of personal data if it wasn't collected directly from you.
- Any details and information of automated decision making, such as profiling, and any meaningful information about the logic involved, as well as the significance and expected consequences of such processing.

To access what personal data is held, identification will be required

We will accept the following forms of ID when information on personal data is requested: a copy of national ID card, driving license, passport, birth certificate and a utility bill not older than three months. A minimum of one piece of photographic ID listed above and a supporting document is required. If we are dissatisfied with the quality, further information may be sought before personal data can be released. All requests should be made to miriam@resolveireland.ie.

Complaints

In the event that you wish to make a complaint about how your personal data is being processed by us, or by our partners, you have the right to complain to Miriam Maher, Managing Director.

If you do not get a response within 30 days you can complain to the Office of the Data Protection Commissioner, Supervising Authority of Ireland.

Resolve Ireland, November 2023