



RDLC Privacy Policy

1 Introduction

In its everyday business operations, the Recruitment Directors Lunch Club Limited (RDLC) makes use of a variety of data about identifiable individuals, including data about:

Current, past and prospective employees

Members

Users of its websites

Subscribers

Other stakeholders

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps RDLC is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to the RDLC website.

The following policies and procedures are relevant to this document:

- Data Protection Impact Assessment Process
- Personal Data Mapping Procedure
- Legitimate Interest Assessment Procedure
- Information Security Incident Response Procedure
- GDPR Roles and Responsibilities
- Records Retention and Protection Policy

2 Privacy and Personal Data Protection Policy

2.1 The General Data Protection Regulation

The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way that RDLC carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is RDLC's policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

2.2 Definitions

There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

'Personal data' is defined as:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'processing' means:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'controller' means:

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

2.3 Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the GDPR is based.

These are as follows:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the

public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

RDLC will ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

2.4 Rights of the Individual

The data subject also has rights under the GDPR. These consist of:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Each of these rights are supported by appropriate procedures within RDLC that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown in Table 1.

<i>Data Subject Request</i>	<i>Timescale</i>
The right to be informed	When data is collected (if supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling	Not specified

Table 1 – Timescales for data subject requests

2.5 Lawfulness of Processing

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the GDPR. It is Second Home Ltd policy to identify the appropriate basis for processing and to document it, in accordance with the Regulation. The options are described in brief in the following sections.

2.5.1 Consent

Unless it is necessary for a reason allowable in the GDPR, RDLC will always obtain explicit consent from a data subject to collect and process their data. The Services are not directed to children under the age of 16 and we do not knowingly collect personal information from anyone under the age of 16. Where different age limitations apply, we comply with them. Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject then this information will be provided to the data subject within a reasonable period after the data are obtained and definitely within one month.

2.5.2 Performance of a Contract

Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.g. a membership invoice cannot be sent without an email address to deliver to.

2.5.3 Legal Obligation

If the personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector.

2.5.4 Vital Interests of the Data Subject

In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. RDLC will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data. As an example, this may be used in aspects of social care, particularly in the public sector.

2.5.5 Task Carried Out in the Public Interest

Where RDLC needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

2.5.6 Legitimate Interests

If the processing of specific personal data is in the legitimate interests of RDLC and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing.

As an example, when personal data is collected for attending an event at RDLC, we will add attendees to our newsletter about upcoming events. How to unsubscribe, change preferences and access/update data will be clearly defined and accessible on every email communication.

Again, the reasoning behind this view will be documented.

2.6 Privacy by Design

RDLC has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation
- Use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate.

2.7 Contracts Involving the Processing of Personal Data

RDLC will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR. For more information, see the GDPR Controller-Processor Agreement Policy.

2.8 International Transfers of Personal Data

Transfers of personal data outside the European Union will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfers will be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

2.9 Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

2.10 Breach Notification

It is RDLC's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance

with our Information Security Incident Response Procedure which sets out the overall process of handling information security incidents.

Under the GDPR the relevant DPA has the authority to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the regulations.

2.11 Addressing Compliance to the GDPR

The following actions are undertaken to ensure that RDLC complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
 - Organisation name and relevant details
 - Purposes of the personal data processing
 - Categories of individuals and personal data processed
 - Categories of personal data recipients
 - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
 - Personal data retention schedules
 - Relevant technical and organisational controls in place
- These actions are reviewed on a regular basis as part of the management process concerned with data protection.

2.12 Changes to This Privacy Policy in the Future

Privacy laws and guidelines are part of a constantly changing environment. We will notify you of material changes by e-mail or by posting a message on the relevant Services.

3 Cookies, Web Beacons, and other Internet Technologies

We, as well as certain third parties that provide content and other functionality on our Services, use cookies, web beacons and other similar technologies on our online Services.

3.1 Cookies

A cookie is a small file that may be stored on your computer or other device. A cookie enables the entity that put the cookie on your device to recognise it across different websites, services, devices, and browsing sessions.

Our websites use Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses so-called "cookies", text files which are stored on the computer of the user and which help the website analyse how visitors use the site. The information generated by the

cookies about the use of our websites will generally be transmitted to, and stored on, a Google server in the United States. On our websites, the IP-anonymization feature has been activated so that the IP address of Google users within the European Economic Area is truncated beforehand. Only in exceptional cases will the full IP address be transferred to Google in the United States and truncated there. Google will use this information on behalf of the website operator for the purpose of evaluating the use of the website by the users, compiling reports on the website activity and providing other services relating to the website activity and internet usage to the website operator. The IP address which your browser transmits in the framework of Google Analytics will not be associated with any other Google data. You may prevent the storage of the cookies by using a particular browser setting. Please note however that in this case you may not be able to fully use all the functions of our websites. Users may prevent the collection of the data generated by the cookie and related to their use of our websites (including their IP address) and its processing by Google by downloading and installing a Browser-Plugin.

You can object to the use of cookies. When you use a web browser to access the Services, you may configure your browser to accept all cookies, reject all cookies, or notify you when a cookie is sent. Click the “Help” menu of your browser to learn more about how to change your cookie preferences. The operating system of your device may contain additional controls for cookies. Please note that disabling cookies may affect your ability to access and use certain features of the Services.

3.2 Web Beacons

Web beacons and similar technologies are small bits of code, which are embedded in web pages, advertisements, and e-mail, that communicate with third parties. We use web beacons, for example, to count the number of users who have visited a particular web page, to deliver or communicate with cookies, and to understand usage patterns. We also may include web beacons in e-mails to understand whether messages have been opened, acted on, or forwarded.

3.3 Other Technologies

There are other local storage and internet technologies, such as Local Shared Objects (also referred to as “Flash cookies”) and HTML5 local storage, that operate similarly to the cookies discussed above in that they are stored on your device and can be used to store certain information about your activities and preferences across different services and sessions. Please note that these technologies are distinct from cookies, and you may not be able to control them using standard browser tools and settings.

3.4 How We Use These Technologies

Our websites use these technologies for the following purposes:

3.4.1 Administering our Services

3.4.2 Improving our Services

Improving our services, including helping us measure and research the effectiveness of our content, features, advertisements, and other communications. For example, we measure which pages and features website visitors are accessing and how much time they are spending on our webpages. We may include web beacons in e-mails, for example, to understand whether messages have been opened, acted on, or forwarded.

3.4.3 Storage

Storing your sign-in credentials and preferences so that you do not have to enter those credentials and preferences every time you log on to a Service.

3.4.4 Advertising

Helping us provide you with relevant content and advertising by collecting information about your use of our Services and other websites.

4 Questions or Comments

If you have any questions or comments regarding our Policy, please contact us at:

RDLC

Hukletree

18 Finsbury Square

London EC2A 1AH

Email: dean@rdlcpirates.com

Effective Date: May 25th, 2018

5 Membership and Newsletter Sign-Up

This privacy notice tells you about the information we collect from you when you sign up to receive our newsletters via our websites (<https://rdlc.wildapricot.org>). In collecting this information, we are acting as a data controller and, by law, we are required to provide you with information about us, about why and how we use your data, and about the rights you have over your data.

Who are we?

RDLC is the Recruitment Directors Lunch Club Limited. A Private members club for the owners, founders, CEOs and Directors of Recruitment Businesses

We are not required to have a data protection officer, so any enquiries about our use of your personal data should be addressed to the contact details above.

What personal data do we collect?

When you enquire about or become a member of the RDLC, we ask you for your name and your email address.

Why do we collect this information?

We will use your information to send you our newsletters, which contain information about our services and events and information about suppliers with which we have negotiated rates or special services on behalf of our members. We will not share your data with any person, business or body, outside of the RDLC membership and all data shared is anonymised unless permission has been given on a case by case basis to improve the data's relevance.

Your consent to do this is given on becoming a fee-paying member of RDLC, and we will only send you our newsletter for as long as you continue to be a member thus implying consent.

What do we do with your information?

Your information is stored in our database and only with those supplier members with which, on your behalf, we have negotiated exclusive deals (typically cost reduction). We will not use the information to make any automated decisions that might affect you.

How long do we keep your information for?

Your information is kept for as long as you continue to be a fee-paying member or supplier member of RDLC.

Your rights over your information

By law, you can ask us what information we hold about you, and you can ask us to correct it if it is inaccurate.

You can also ask for it to be erased and you can ask for us to give you a copy of the information.

You can also ask us to stop using your information – the simplest way to do this is to withdraw your consent, which you can do at any time, by emailing, writing or telephoning us using the contact details above.

Your right to complain

If you have a complaint about our use of your information, you can contact the Information Commissioner's Office via their website at www.ico.org/concerns or write to them at:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

6 Recruitment Privacy Policy

As part of any recruitment process, RDLC collects and processes personal data relating to job applicants. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information do we collect?

RDLC collects a range of information about you. This includes: your name, address and contact details, including email address and telephone number; details of your qualifications, skills, experience and employment history; information about your current level of remuneration, including benefit entitlements; whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process; and information about your entitlement to work in the UK.

RDLC may collect this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment. We may also collect personal data about

you from third parties, such as references supplied by former employers. We will seek information from third parties only once a job offer to you has been made and will inform you that we are doing so. Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why does RDLC process personal data?

We need to process data to take steps at your request prior to entering into a contract with you. We may also need to process your data to enter into a contract with you. In some cases, we need to process data to ensure that we are complying with its legal obligations. For example, it is mandatory to check a successful applicant's eligibility to work in the UK before employment starts.

RDLC has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. We may also need to process data from job applicants to respond to and defend against legal claims.

RDLC may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics. We may also collect information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. We process such information to carry out its obligations and exercise specific rights in relation to employment. If your application is unsuccessful, RDLC may keep your personal data on file in case there are future employment opportunities for which you may be suited. We will ask for your consent before keeping your data for this purpose and you are free to withdraw your consent at any time.

Who has access to data?

Your information may be shared internally for the purposes of the recruitment exercise. This includes interviewers involved in the recruitment process, managers in the business area with a vacancy. We will not share your data with third parties unless your application for employment is successful and we make you an offer of employment. We will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks.

How does RDLC protect data?

We take the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

For how long does RDLC keep data?

If your application for employment is unsuccessful, the organisation will hold your data on file for 6 (six) months after the end of the relevant recruitment process. If you agree to allow us to keep your personal data on file, we will hold your data on file for a further 6 (six) months for consideration for future employment opportunities. At the end of that period, or once you withdraw your consent, your data is deleted or destroyed. You will be asked when you submit your CV whether you give us consent to hold your details for the full 12 months in order to be considered for other positions or not.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your Human Resources file (electronic based) and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- and object to the processing of your data where Second Home is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact emma@rdlcpirates.com

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to RDLC during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all.