

McCARTHY TÉTRAULT: RECRUITMENT PRIVACY NOTICE

This notice

1. Like most businesses, McCarthy Tétrault holds and processes a wide range of information, some of which relates to individuals who are applying to work for or with us. This Privacy Notice explains the type of information we process, why we are processing it and how that processing may affect you, when you apply for a position with McCarthy Tétrault's London Office.
 - This Privacy Notice focuses on individuals who are applying to work for or with us and the data we process as part of the recruitment process, including the following purposes: To assess your suitability for any position for which you may apply for at McCarthy Tétrault (or future positions for which we think you may be suitable), including applications that we receive online, via email or by hard copy or in person.
 - To review McCarthy Tétrault's equal opportunities profile in accordance with the requirements of the Solicitors Regulation Authority, and to ensure that McCarthy Tétrault does not discriminate on the grounds of gender, race, ethnic origin, age, religion, sexual orientation, disability or any other basis. All recruitment decisions are made entirely on merit.

We have a separate Workplace Privacy Notice that applies to our current and former employees.

2. This Privacy Notice is set out in this document (the Core Notice) and the Supplementary Information in Annex 1 to this document. In the Supplementary Information, we explain what we mean by "personal data", "processing", "special personal data" and other terms used in the notice.
3. In brief, this Privacy Notice explains:
 - what personal data we hold and why we process it;
 - the legal grounds which allow us to process your personal data;
 - where the data comes from, who gets to see it and how long we keep it;
 - how to access your personal data and other rights; and
 - how to contact us.

Personal data – what we hold and why we process it

4. We process data for the purposes of our business including recruitment, management, administrative, employment/engagement and legal purposes. The Supplementary Information provides more specific information on these purposes, on the type of data that may be processed and on the grounds on which we process data. See *Legal grounds for processing personal data* and *Further information on the data we process and our purposes*.

Where the data comes from and who gets to see it

5. Some of the personal data that we process about you comes from you. For example, you tell us your contact details and work history. If you are joining us, you may provide your banking details.
6. Other personal data may come from third parties such as recruiters acting on your behalf or from your references.

7. Your personal data will be seen internally by managers, HR and, in some circumstances (particularly, if you join us) by colleagues in members of our group in Canada and the US. We will, where necessary and as set out in this Privacy Notice, also pass your data outside the organisation, for example to people you are dealing with and payroll agencies. Further information on this is provided in the Supplementary Information. See *Where the data comes from* and *Who gets to see your data?*

How long do we keep your personal data?

8. We do not keep your personal data for any specific period, but will not keep it for longer than is necessary for our purposes. In general, if you become employed by or engaged with us, we will keep your personal data for the duration of that relationship and for a period afterwards. If you are unsuccessful in gaining employment with us, we will likely keep your personal data for a short period after informing you that you were unsuccessful. See *Retaining your personal data – more information* in the Supplementary Information.

Transfers of personal data outside the EEA

9. We will, where necessary and as set out in this Privacy Notice, transfer your personal data outside the UK (United Kingdom) and/or the EEA (European Economic Area) to members of our group in Canada and the US who are involved in the application process. Further information on these transfers and the measures taken to safeguard your data are set out in the Supplementary Information under *Transfers of personal data outside the UK and/or the EEA – more information*.

Your data rights

10. You have a right to make a subject access request to receive information about the data that we process about you. Further information on this and on other rights is in the Supplementary Information under *Access to your personal data and other rights*. We also explain how to make a complaint about our processing of your data.

Contact details

11. In processing your personal data, we act as a data controller. Our contact details are as follows:
Antje Dilger – Manager, Finance and Human Resources – *London, UK Office*
Robert Brant – Managing Partner – *London, UK Office*
<https://www.mccarthy.ca/en/contact-us/london-uk>

Status of this notice

12. This notice does not form part of any contract of employment you might enter into, and does not create contractual rights or obligations. It may be amended by us at any time. Nothing in this Privacy Notice is intended to create an employment relationship between McCarthy Tétrault and any non-employee.

ANNEX 1

SUPPLEMENTARY INFORMATION

What do we mean by “personal data” and “processing”?

1. “Personal data” is information relating to you (or from which you may be identified) which is processed by automatic means or which is (or is intended to be) part of a structured manual filing system. It includes not only facts about you, but also intentions and opinions about you.
2. Data “processed automatically” includes information held on, or relating to use of, a computer, laptop, mobile phone or similar device. It covers data derived from equipment such as access passes within a building, data on use of vehicles and sound and image data such as CCTV or photographs.
3. “Processing” means doing anything with the data. For example, it includes collecting it, holding it, disclosing it and deleting it.
4. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sexual orientation, sex life, trade union membership and genetic and biometric data are subject to special protection and considered by EU privacy law to be “special personal data”.
5. References in this Privacy Notice to employment, work (and similar expressions) include any arrangement we may have under which an individual provides us with work or services, or applies for such work or services. By way of example, when we mention an “employment contract”, that includes a contract under which you provide us with services; when we refer to ending your potential employment, that includes terminating a contract for services.

We use the word “you” to refer to anyone within the scope of the notice.

LEGAL GROUNDS FOR PROCESSING PERSONAL DATA

What are the grounds for processing?

6. Under data protection law, there are various grounds on which we can rely when processing your personal data. In some contexts more than one ground applies. We have summarised these grounds as Contract, Legal obligation, Legitimate Interests and Consent and outline what those terms mean in the following table.

| Term | Ground for processing | Explanation |
|----------------------|---|--|
| Contract | Processing necessary for performance of a contract with you or to take steps at your request to enter a contract. | This covers carrying out our contractual duties and exercising our contractual rights. |
| Legal obligation | Processing necessary to comply with our legal obligations. | Ensuring we perform our legal and regulatory obligations. For example, providing a safe place of work and avoiding unlawful discrimination. |
| Legitimate Interests | Processing necessary for our or a third party's legitimate interests. | We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests processing your data. |

| Term | Ground for processing | Explanation |
|---------|--|---|
| | | Your data will not be processed on this basis if our or a third party's interests are overridden by your own interests, rights and freedoms. |
| Consent | You have given specific consent to processing your data. | In general processing of your data in connection with employment is not conditional on your consent. But there may be occasions where we do specific things such as provide a reference and rely on your consent to our doing so. |

Processing special personal data

7. Processing special data about you may be necessary (for example, storing your health records to assist us in ensuring that we provide you with a healthy and safe workplace, or processing personal data relating to diversity monitoring). Our Appropriate Policy Document, which covers such processing carried out in the UK, can be found at Annex 2. If we process your special data, we will also make sure that one or more of the grounds for processing special personal data applies. In outline, these include:

- Processing being necessary for the purposes of your or our obligations and rights in relation to our working relationship in so far as it is authorised by law or collective agreement;
- Processing relating to data about you that you have made public (e.g. if you tell colleagues and/or individuals at McCarthy Tétrault that you are ill);
- Processing being necessary for the purpose of establishing, making or defending legal claims;
- Processing being necessary for provision of health care or treatment, medical diagnosis, and assessment of your working capacity; and
- Processing for equality and diversity purposes to the extent permitted by law.

Further information on the data we process and our purposes

8. The Core Notice outlines the purposes for which we process your personal data. More specific information on these, examples of the data and the grounds on which we process data are in the table below.
9. The examples in the table cannot, of course, be exhaustive. For example, although the table does not mention data relating to criminal offences, if we were to find out that someone applying to work for us was suspected of committing a criminal offence, we might process that information if relevant for our purposes. If necessary we will also require criminal background checks for certain roles – for example those working in financial roles.

| Purpose | Examples of personal data that may be processed | Grounds for processing |
|-------------|--|------------------------------|
| Recruitment | Standard data related to your identity (e.g. your name, address, email address, identity information and documents, telephone numbers, place of birth, nationality, contact details, professional experience | Contract Legal obligation |

| Purpose | Examples of personal data that may be processed | Grounds for processing |
|---|--|--|
| | <p>and education (including university degrees, academic records, professional licenses, memberships and certifications, awards and achievements, and current and previous employment details), financial information (including current salary information), language skills), and any other personal data that you present us with as part of your application related to the fulfilment of the role.</p> <p>Information concerning your application and our assessment of it, your references, any checks we may make to verify information provided or background checks and any information connected with your right to work.</p> <p>If necessary, we will also process information concerning your health, any disability and in connection with any adjustments to working arrangements.</p> | Legitimate interests |
| Administering our recruitment process | <p>Evaluating your experience and qualifications against the requirements of the position you are applying for.</p> <p>Administering our online careers portal.</p> <p>Communicating with you in respect of any offer of employment we choose to make and providing you with information about our onboarding process.</p> | Contract Legal obligation Legitimate interests |
| Entering into a contract with you (if you are made an offer by us) | Information on your terms of employment from time to time, including your hours and working patterns, pay and benefits, such as your participation in pension arrangements, life and medical insurance; and any bonus or share schemes. | Contract Legal obligation Legitimate interests |
| Contacting you or others on your behalf | Your address and phone number, emergency contact information and information on your next of kin. | Contract Legitimate interests |
| Payroll administration <i>(for employees and workers only)</i> | Information on your bank account, pension contributions and on tax and national insurance Your national insurance number or other government issued identifier. | Contract Legal obligation Legitimate interests |
| Financial planning and budgeting <i>(for employees and workers only)</i> | Information such as your proposed salary and (if applicable) envisaged bonus levels. | Legitimate interests |

| <i>Purpose</i> | <i>Examples of personal data that may be processed</i> | <i>Grounds for processing</i> |
|---|--|--|
| Physical and system security | CCTV images upon attendance for interview at our premises. | Legal obligation Legitimate interests |
| Providing information to third parties in connection with transactions that we contemplate or carry out | Information on any offer made to you and your proposed contract and other employment data that may be required by a party to a transaction such as a prospective purchaser, seller or outsourcer. | Legitimate interests |
| Monitoring of diversity and equal opportunities | Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability and age as part of diversity monitoring initiatives. Such data will be aggregated and used for equality of opportunity monitoring purposes. Please note we may share aggregated and anonymised diversity statistics with regulators if formally required / requested. | Legitimate interests |
| Disputes and legal proceedings | Any information relevant or potentially relevant to a dispute or legal proceeding affecting us. | Legitimate interests Legal obligation |
| Meeting our duty of care and health and safety responsibilities in relation to Covid-19 | We have a duty of care to ensure a safe place of work, as well as a duty of care to staff. For this reason, where reasonable and necessary, we may do the following in relation to Covid-19, before requesting an in-person interview: <ul style="list-style-type: none"> • request information about whether you have had symptoms of the virus, close contact with confirmed cases or travelled to high risk areas, whether you would be considered clinically vulnerable or clinically extremely vulnerable and whether you have been vaccinated; • conduct temperature checks before allowing entrance to our premises; • ask you to be PCR or Antibody tested before allowing entrance to our premises; and/or • ask you to provide us with your proof of vaccination against Covid-19 (or ask for other similar information related to the NHS Covid Pass) before allowing entrance to our premises. | Legal obligation Legitimate interest: to ensure a safe place of work and the safety of our staff Article 9(2) GDPR condition: processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment, or where it is in the public interest to do so |

| Purpose | Examples of personal data that may be processed | Grounds for processing |
|--------------------------------|---|------------------------|
| If relevant, Regulatory issues | For instance, complying with requirements set out by the Solicitors Regulation Authority. | Legal obligation |

10. Please note that if you accept an offer from us, McCarthy Tétrault will process further information as part of the employment relationship. We will provide you with our full *Workplace Privacy Notice* as part of the on-boarding process.

Where the data comes from

11. When you apply to work for or with us, the initial data about you that we process is likely to come from you: for example, contact details, bank details and information on your immigration status and whether you can lawfully work. Where necessary and in accordance with this privacy notice, we will require references and information to carry out background checks. If you have concerns about this in a particular context, you should speak to your recruiter or the Managing Partner.
12. Please note we may also receive data from third party recruiters, agents and similar organisations as a part of the recruitment process.

WHO GETS TO SEE YOUR DATA?

Internal use

13. Where necessary and as set out in this Privacy Notice, your personal data will be disclosed to relevant managers and administrators for the purposes of your application as mentioned in this document. We will also disclose this to members of our group in Canada and the US where necessary for decision making regarding your application – this will depend on the type of role you are applying for.

External use

14. We will only disclose your personal data outside McCarthy Tétrault if disclosure is consistent with a ground for processing on which we rely and doing so is lawful and fair to you.
15. We will disclose your data if it is necessary for our legitimate interests as an organisation or the interests of a third party (but we will not do this if these interests are over-ridden by your interests and rights, in particular, to privacy). Where necessary, we will also disclose your personal data if you consent, where we are required to do so by law and in connection with criminal or regulatory investigations.
16. Specific circumstances in which your personal data may be disclosed include:
- Disclosure to organisations that process data on our behalf such as our payroll service, insurers and other benefit providers, our bank and organisations that host our IT systems and data. This would normally occur if you accept an offer from us and would be carried out as part of the on-boarding process;
 - To third party recruitment consultants and similar businesses (including online recruitment portals) as a part of the recruitment process;
 - Disclosure of aggregated and anonymised diversity data to relevant regulators as part of a formal request (see above); and
 - To third parties for the purpose of assessing efficiency of mobile device usage (as detailed above) on an anonymised basis.

Retaining your personal data – more information

17. Although there is no specific period for which we will keep your personal data, we will not keep it for longer than is necessary for our purposes. In general, if you are successful in becoming employed by us, we will keep your personal data for the duration of the your employment and for a period afterwards. If you are unsuccessful in gaining employment with us, we will likely keep your personal data for a short period after informing you that you were unsuccessful. In considering how long to keep your data, we will take into account its relevance to our business and your potential employment/engagement either as a record or in the event of a legal claim.
18. If your data is only useful for a short period (for example, CCTV footage data) we will delete it.
19. Personal data relating to job applicants (other than the person who is successful) will normally be deleted after 12 months.

Transfers of personal data outside the UK and/or the EEA – more information

20. In connection with our business and for employment/engagement, administrative, management and legal purposes, we will, where necessary and as set out in this Privacy Notice, transfer your personal data outside the UK and EEA to members of our group assisting with the recruitment process in Canada and the US). We will ensure that any transfer is lawful and that there are appropriate security arrangements.
21. We have entered into an agreement ensuring that appropriate and suitable safeguards are in place with members of our group. If you wish to see details of these safeguards, please ask the Chief Information Officer.

Access to your personal data and other rights

22. We try to be as open as we reasonably can about personal data that we process. If you would like specific information, just ask us.
23. You also have a legal right to make a “subject access request”. If you exercise this right and we hold personal data about you, we are required to provide you with information on it, including:
 - Giving you a description and copy of the personal data; and
 - Telling you why we are processing it.
24. If you make a subject access request and there is any question about who you are, we may require you to provide information from which we can satisfy ourselves as to your identity.
25. As well as your subject access right, you may have a legal right to have your personal data rectified or erased, to object to its processing or to have its processing restricted. If you have provided us with data about yourself (for example your address or bank details), you have the right to be given the data in machine readable format for transmitting to another data controller. This only applies if the ground for processing is Consent or Contract.
26. If we have relied on consent as a ground for processing, you may withdraw consent at any time – though if you do so that will not affect the lawfulness of what we have done before you withdraw consent.

Complaints

27. If you have complaints relating to our processing of your personal data, you should raise these with the Managing Partner in the first instance. You may also raise complaints with your statutory regulator. For contact and other details ask the Managing Partner.

Status of this notice

28. This notice does not form part of any contract of employment that you may enter into with you and does not create contractual rights or obligations. It may be amended by us at any time. Nothing in this notice is intended to create an employment relationship between McCarthy Tétrault and any non-employee.

ANNEX 2

APPROPRIATE POLICY DOCUMENT

Please note that this Workplace Privacy Notice (including the information detailed below), along with other related policies and/or protocols, shall form our policy for processing special data and criminal convictions data as required by the UK Data Protection Act 2018 (Schedule 1 Part IV).

Description of special data processed:

- nationality, racial and ethnic origin, gender, sexual orientation, religion, disability age, and data concerning health. We also process criminal convictions data as part of the hiring process for certain roles.

Schedule 1 conditions for processing:

- processing is necessary for reasons of substantial public interest relating to equality of opportunity or treatment (Schedule 1 Part II section 8(1) UK Data Protection Act 2018);
- processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller in connection with employment (Schedule 1 Part I section 1 UK Data Protection Act 2018).

• Procedures for ensuring compliance with the principles:

• Accountability principle:

- We maintain appropriate documentation of our processing activities, as set out in our Article 30 record of processing
- We have appropriate data protection policies in place, such as Data Breach Policy and its supporting policies, guideline and documents;
- We carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests.

• Principle (a): lawfulness, fairness and transparency:

- We identify an appropriate lawful basis for processing and a further Schedule 1 condition for processing special data, as set out in this Workplace Privacy Notice;
- We make appropriate privacy information available with respect to the special data, as set out in this Workplace Privacy Notice;
- We are open and honest when we collect the special data and we ensure we do not deceive or mislead people about its use, by making this Workplace Privacy Notice available.

• Principle (b): purpose limitation

- We have clearly identified our purposes for processing the special data, as set out in this Workplace Privacy Notice;
- We have included appropriate details of these purposes in our privacy information for individuals, as set out in this Workplace Privacy Notice;
- If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), we either check that this is compatible with our original purpose

or where we have another lawful basis, be transparent about this new processing or get specific consent for the new purpose

- **Principle (c): data minimisation**

- We are satisfied that we only collect special personal data we actually need for our specified purposes;
- We are satisfied that we have sufficient special data to properly fulfil those purposes;
- We periodically review this particular special data, and delete anything we don't need.

- **Principle (d): accuracy**

- We have appropriate processes in place to check the accuracy of the special data we collect, and we record the source of that data
- We have a process in place to identify when we need to keep the special data updated to properly fulfil our purpose, and we update it as necessary;

- **Principle (e): storage limitation**

- We carefully consider how long we keep the special data and we can justify this amount of time;
- We regularly review our information and erase or anonymise this special data when we no longer need it;
- We have clearly identified any special data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

- **Principle (f): integrity and confidentiality (security)**

- We have analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data;
- We have an IT Communications and IT Monitoring Policy and we take steps to make sure the policy is implemented.
- We have put other technical measures or controls in place because of the circumstances and the type of special data we are processing

Retention and erasure policies

See our Data Retention Policy.