Delete this page from the policy given to the employee/client

Template policy - DP5: Privacy Notice (including for use on the company’s website)

|  |
| --- |
| V2: October 2022 |

Guidance note

The UK General Data Protection Regulation (GDPR) requires organisations to be more transparent with individuals about the personal data they hold, why they hold it and what they plan to do with it. To do this, data controllers must provide specific information to data subjects when first collecting their personal data – this is known as ‘transparency information’. One of the ways to provide this information is through a privacy notice. This can be done in paper or electronic form e.g. by PDF or email and/or a pre-recorded message.

This is an example of a privacy notice that you may find useful as the basis for writing your own privacy notice. We recommend that you speak with your IT/ CRM providers about any specific references to software such as in sections 6, 7 and 8. You will need to tailor the document to reflect your own organisation’s practices. Unfortunately, the REC Legal team does not provide a document review service.

Why we updated this document

This is a new Privacy Notice. We previously had separate privacy notices for when data is collected directly from the individual (DP5A) and when it is collected from a third party (DP5B). As we drafted this privacy statement (which is for use on the company’s website) we decided to merge all three documents together for ease. However, members can still use separate documents if they wish.

Why do you need a privacy statement?

The UK General Data Protection Regulation (GDPR) requires organisations to be more transparent with individuals about the personal data they hold, why they hold it and what they plan to do with it. To do this, data controllers must provide specific information to data subjects when first collecting their personal data – this is known as ‘transparency information’. One of the ways to provide this information is through a privacy notice. This can be done in paper or electronic form e.g. by PDF or email, or individuals can be directed to the company’s website or a pre-recorded message. The ICO has also issued guidance which states that it is best practice to issue the privacy notice using the same medium through which you collected the data. Therefore, if collecting data in paper form e.g. via registration form, then give the privacy notice in paper form. Similarly, if collecting data via the website then direct the individual to the privacy notice on the website.

When to give the transparency information

At all times when considering when to provide the transparency information, **you must consider the reasonable expectations of the individual, the effects the processing will have on him or her and the individual’s ability to exercise his or her rights**. Importantly, accountability requires transparency across the whole processing life cycle and not just at the initial point of contact so you must tell individuals about any changes to processes or privacy notices.

|  |  |
| --- | --- |
| How you collect the data | When to give the privacy statement |
| 1. You collect the personal data from the individual directly (e.g. on a registration form or via the company website). | You should give the transparency information when you first collect the personal data. |
| 1. You do not collect the personal data from the data subject directly (e.g. where you collect it from a third party data controller such as a jobs board, or from another data subject or a public source). | When you collect data from sources other than the individual concerned you must tell him/ her (a) what personal data you collected about them and (b) where you obtained the data from. You must do this no later than one month after you collected the data, or when you first communicate with the data subject if that is before one month expires. If you disclose the personal data to a third party before the one month expires, then you must give the transparency information no later than the first disclosure. |

Keeping the information up to date

More detailed advice on GDPR is available on the [REC Legal guide](https://www.rec.uk.com/recruiters/legal/legal-guide/data-protection). You will need your login details to access this. All hyperlinks in this checklist are correct at the time of writing.

Suite of model data protection documents

We have produced a suite of model documents and guidance to be used for data protection purposes. They include:

[DP1 – GDPR checklist](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/model-document-dp1-gdpr-checklist)

[DP2 – Matrix of legal bases for processing and documents to use](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/document-dp2-matrix-sources-personal-data-legal-bases-and-documents-use)

[DP3 – Data protection policy](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/data-protection-policy)

[DP4 – Data protection procedure](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/data-protection-procedure)

[DP5 - Privacy Notice](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/model-document-dp5-privacy-notice-including-use-companys-website) (including for use on the company’s website)

[DP5A – Privacy notice (when personal data is obtained from the data subject)](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/model-document-dp5a-privacy-notice-when-personal-data-obtained-directly-data-subject)

[DP5B – Privacy notice (when personal data is not obtained from the data subject)](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/model-document-dp5b-example-privacy-notice-you-may-find-useful-basis-writing-your-own-privacy-notices)

[DP6 – Consent form](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/model-document-dp6-consent-form)

[DP7 – Withdrawal of consent form](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/model-document-dp7-withdrawal-consent-form)

[Infographic for jobseekers – know your data protection rights](https://www.rec.uk.com/recruiters/legal/legal-resources/eu-general-data-protection-regulation-gdpr/understand-your-data-protection-rights)

[A Guide to the EU General Data Protection Regulation](https://www.rec.uk.com/recruiters/legal/legal-resources/eu-general-data-protection-regulation-gdpr/rec-guide-eu-general-data-protection-regulation)

[Record keeping table](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/record-keeping-table)

Please see the [Model Document Library](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection?&pageId=6236&search=&sortBy=A%20-%20Z&page=1) for a complete list of REC model documents.

See also the [ICO Guidance on UK GDPR](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/), [ICO Guidance on legitimate interest](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/) and the [ICO legal basis interactive tool](https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/lawful-basis-interactive-guidance-tool/).

How to use this model document

This form can be made available on your website as your privacy notice but should not be used as your website privacy statement. A website privacy statement should include details of the different types of information processed through your website e.g. cookies and tracking information.

Notes: All notes are at the back of the policy. We suggest you print the notes separately so that you can read them side by side with the policy (rather than flick back and forth through the text). Delete all “[*see Note X*]” from the text when finalising the policy.

**Highlighting:** In order to assist you in using this template for your own business’ needs we have highlighted the places where you will need to insert information specific to your business and also in the explanatory notes at the end of the template policy. The notes and insertions are highlighted in grey. To remove highlighting from your Word document select the highlighted text, or press CTRL+A to select all of the text in the document; then on the Formatting toolbar, click the arrow next to Highlight tab and then select None to remove the highlighting.

**Options in clauses:** Some clauses require you to choose from Option A or Option B. We have highlighted those options in colour. When you have chosen the appropriate option for your business, simply delete the other option (remember also to remove the letter “A” or “B” from the chosen option).

**Heading and copyright notice:** These should be deleted from your document. To do this click on “View”, “Header & Footer”, a separate toolbar opens allowing you to switch between the header and footer. Select wording in the header or footer and press “Delete”. Then click “Close” in the toolbar.

REC template documents have been prepared exclusively for REC Corporate Members. You must not distribute these template documents to third parties except where you require them to complete the document.

### [Insert the Company logo if desired]

|  |  |
| --- | --- |
| Company Name: | [insert your company name] (‘the Company’) [NOTE 1] |
| Company contact details: | [insert the contact details of the data protection lead in the Company. [NOTE 1] |
| Document DP5 | Privacy Notice (including for use on the company website |
| **Topic:** | Data protection |
| **Date:** | [insert date policy adopted] |
| **Version:** | [insert version no.] |

The Company is a recruitment business which provides work-finding services to its clients and work-seekers. The Company must process personal data (including special categories of personal data) so that it can provide these services – in doing so, the Company acts as a data controller.

You may give your personal details to the Company directly, such as on an application or registration form or via our website, or we may collect them from another source such as a jobs board. The Company must have a legal basis for processing your personal data. For the purposes of providing you with work-finding services and/or information relating to roles relevant to you, we will only use your personal data in accordance with this privacy statement. We will comply with current data protection laws at all times.

### Contents

1. Collection and use of personal data
   1. Purpose of processing and legal basis
   2. Legitimate interest
   3. Statutory/contractual requirement
   4. Recipients of data
2. Information to be provided when data is not collected directly from the data subject
   1. Categories of data
   2. Sources of data
3. Overseas transfers
4. Data retention
5. Your rights
6. Automated decision making
7. Cookies
8. Login files
9. Links to external sites
10. Sale of the business
11. Data security
12. Changes to this privacy statement
13. Complaints or queries

### 1. Collection and use of personal data

1. **Purpose of processing and legal basis** [NOTE 2]

The Company will collect your personal data (which may include special categories of personal data) and will process your personal data for the purposes of providing you with work-finding services. This includes for example, contacting you about job opportunities, assessing your suitability for those opportunities, updating our databases, putting you forward for job opportunities, arranging payments to you and developing and managing our services and relationship with you and our clients.

[If you have opted-in we may also send you marketing information and news via email/text. You can opt-out from receiving these at any time by clicking “unsubscribe” when you receive these communications from us.] [NOTE 3]

On some occasions we may be required to use your data for the purpose of investigating, reporting and detecting crime and also to comply with laws that apply to us. We may also use your information during the course of internal audits to demonstrate our compliance with certain industry standards.

We must have a legal basis to process your personal data. The legal bases we rely upon to offer our work-finding services to you are:

* Your consent [NOTE 4]
* Where we have a legitimate interest [NOTE 5]
* To comply with a legal obligation that we have
* To fulfil a contractual obligation that we have with you
* [insert any other legal basis that you rely on to process the data]

1. **Legitimate interest** [NOTE 5]

This is where the Company has a legitimate reason to process your data provided it is reasonable and does not go against what you would reasonably expect from us. Where the Company has relied on a legitimate interest to process your personal data our legitimate interests is/are as follows:

* Managing our database and keeping work-seeker records up to date;
* Providing work-finding services to you and our clients;
* Contacting you to seek your consent where we need it;
* Giving you information about similar products or services to those that you will have used from us recently;
* [Set out any other legitimate interest for processing the data]

1. **Statutory/contractual requirement** [NOTE 6]

The Company has certain legal and contractual requirements to collect personal data (e.g. to comply with the Conduct of Employment Agencies and Employment Businesses Regulations 2003, immigration and tax legislation, and in some circumstances safeguarding requirements). Our clients may require this personal data, and we may need your data to enter into a contract with you. If you do not give us the personal data we need to collect In order to comply with our statutory and legal requirements, we may not be able to continue to provide work-finding services to you. [set out any other consequences of failure to provide the data].

1. **Recipient/s of data** [NOTE 7]

The Company will process your personal data and/or sensitive personal data with the following recipients:

* Clients (who we may introduce or supply you to)
* Your former employers who we may seek references from
* Payroll service providers who manage payroll on our behalf or other payment intermediaries who we may introduce you to
* Other recruitment agencies in the supply chain
* Auditors who are assessing the compliance and processes of the business to ensure its adherence to all relevant legislation and good practice guidance
* [Insert the identity of other recipients/category of recipients]

### 2. Information to be provided when data collected not from the data subject] [NOTE 8]

**Categories of data:** The Company has collected the following personal data on you:

*Personal data:* [not an exhaustive list – please complete]

* Name, address, mobile no., email
* National insurance no.
* Nationality (through right to work check)
* [Specify any other data…]

*Special categories of personal data:* [not an exhaustive list – please complete]

* [Health information including whether you have a disability]
* [Criminal conviction(s)]
* [Specify any other data…]

Source of the personal data: The Company sourced your personal data/special categories of personal data: [not an exhaustive list – please complete]

* From [name] jobs boards, LinkedIn [NOTE 9]
* A former employer [name]
* A referee whose details you previously provided to us [name]
* Software providers who we use to support our services including [list]
* Cookies listed in section 7
* [Specify any other means by which you obtained the individual’s data]

This information [came/did not come] from a publicly accessible source.

### 3. Overseas Transfers [Optional]

The Company may transfer the information you provide to us to countries outside the UK and/or the European Economic Area (‘EEA’) for the purposes of providing you with work-finding services. We will take steps to ensure adequate protections are in place to ensure the security of your information. The EEA comprises the EU member states plus Norway, Iceland and Liechtenstein.

Or

The Company will not transfer the information you provide to us to countries outside the UK and/or the European Economic Area (‘EEA’) for the purposes of providing you with work-finding services. The EEA comprises the EU member states plus Norway, Iceland and Liechtenstein. [NOTE 10]

### 4. Data retention

The Company will retain your personal data only for as long as is necessary for the purpose we collect it. Different laws may also require us to keep different data for different periods of time. For example, the Conduct of Employment Agencies and Employment Businesses Regulations 2003, require us to keep work-seeker records for at least one year from (a) the date of their creation or (b) after the date on which we last provide you with work-finding services. We are required to keep your records relating to the right to work in the UK 2 years after employment or the engagement has ended alterable and working time records including your 48 hour opt out notice annual leave/holiday records 2 years from the time they were created.

Additionally, we must also keep your payroll records, holiday pay, sick pay and pensions auto-enrolment records for as long as is legally required by HMRC and associated national minimum wage, social security and tax legislation. This is currently 3 to 6 years.

Where the Company has obtained your consent to process your [personal/[and] special categories of personal data/specify which personal data], we will do so in line with our retention policy [([a copy of which is attached](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/model-document-dp9-retention-policy))]. Upon expiry of that period the Company will seek further consent from you. Where consent is not granted the Company will cease to process your [personal data/[and] sensitive personal] data]. [NOTES 11 and 12]

[Add any other retention periods for personal data/[and] sensitive personal data you have not already mentioned above].

### 5. Your rights

Please be aware that you have the following data protection rights:

* The right to be informed about the personal data the Company processes on you;
* The right of access to the personal data the Company processes on you;
* The right to rectification of your personal data;
* The right to erasure of your personal data in certain circumstances;
* The right to restrict processing of your personal data;
* The right to data portability in certain circumstances;
* The right to object to the processing of your personal data that was based on a public or legitimate interest;
* The right not to be subjected to automated decision making and profiling; and
* The right to withdraw consent at any time.

Where you have consented to the Company processing your [personal data/[and]sensitive personal data] you have the right to withdraw that consent at any time by contacting [insert the identity and contract details of the person in your organisation who handles data protection issues and, where applicable, any representative of the controller and the data protection officer]. Please note that if you withdraw your consent to further processing that does not affect any processing done prior to the withdrawal of that consent, or which is done according to another legal basis. [NOTE 13]

There may be circumstances where the Company will still need to process your data for legal or official reasons. Where this is the case, we will tell you and we will restrict the data to only what is necessary for those specific reasons.

If you believe that any of your data that the Company processes is incorrect or incomplete, please contact us using the details above and we will take reasonable steps to check its accuracy and correct it where necessary.

**You can also contact us using the above details if you want us to restrict the type or amount of data we process for you, access your personal data or exercise any of the other rights listed above.**

### 6. Automated decision-making [Optional] [NOTE 14]

[If your Company uses automated decision-making, including profiling, you must give meaningful information about the process, as well as the significance and the effect of such processing for the individual.]

### 7. Cookies [NOTE 15]

We may obtain data about you from cookies. These are small text files that are placed on your computer by websites that you visit. They are widely used to make websites work, or work more efficiently, as well as to provide information to the owners of the site. Cookies also enable us to deliver more personalised content.

The table below explains the cookies we use and why.

|  |  |  |  |
| --- | --- | --- | --- |
| Cookie | Name | Purpose | More information |
|  |  |  |  |

Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, [please refer to our Cookie policy]. [Please note that in a few cases some of our website features may not function if you remove cookies from your browser.]

### 8. Login Files

We use IP addresses to analyse trends, administer the site, track users’ movements, and to gather broad demographic information for aggregate use. IP addresses are not linked to personally identifiable information.

### 9. Links to external websites

The Company’s website may contain links to other external websites. Please be aware that the Company is not responsible for the privacy practices of such other sites. When you leave our site we encourage you to read the privacy statements of each and every website that collects personally identifiable information. This privacy statement applies solely to information collected by the Company’s website.

### 10. Sale of business

If the Company’s business is sold or integrated with another business your details may be disclosed to our advisers and any prospective purchasers and their advisers and will be passed on to the new owners of the business. Where the sale of the business results in the transfer of your details to a different data controller we will notify you of this.

### 11. Data Security

The Company takes every precaution to protect users’ information. [insert details of security measures in relation to the personal data processed, e.g. firewalls, browser certification technology, encryption, limited access, use of passwords etc. as appropriate].

Only employees who need the information to perform a specific job (for example, consultants, our accounts clerk or a marketing assistant) are granted access to your information.

The Company uses all reasonable efforts to safeguard your personal information. However, you should be aware that the use of email/ the Internet is not entirely secure and for this reason the Company cannot guarantee the security or integrity of any personal information which is transferred from you or to you via email/the Internet.

If you share a device with others, we recommend that you do not select the “remember my details” function when that option is offered.

**If you have any questions about the security at our website, you can email [insert name and email address].**

### 12. Changes to this privacy statement

We will update this privacy statement from time to time. We will post any changes on the statement with revision dates. If we make any material changes, we will notify you.

### 13. Complaints or queries [NOTE 16]

If you wish to complain about this privacy notice or any of the procedures set out in it please contact: [insert the identity and contract details of the person in the Company who handles data protection issues and, where applicable, any representative of the controller and the data protection officer].

You also have the right to raise concerns with the Information Commissioner’s Office on 0303 123 1113 or at <https://ico.org.uk/make-a-complaint/>, or any other relevant authority should your personal data be processed outside of the UK and you believe that your data protection rights have not been adhered to.

NOTES – delete these notes from the privacy notice when published

|  |  |  |
| --- | --- | --- |
| Note no. | Section no. | Explanation |
|  | Company name/contact details | You must include the identity and contact details of your company, any of the controller’s representatives and the data protection officer where applicable.  A “representative” for this purpose is an external individual or company based in the EU who you have appointed to represent your organisation regarding your obligations under the UK GDPR. |
|  | Purpose of processing | You must confirm why you will process the personal data and the legal basis you are relying on for processing the data. The six lawful bases to process personal data and special categories of personal data can be found at Annex A.  N.B. Annex A is for reference purposes only, it does not need to be included in the privacy notice and can be deleted from this document.  The ICO has produced a [legal basis interactive tool](https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/lawful-basis-interactive-guidance-tool/) which may assist you. |
|  | Marketing information | See the [DP8 Marketing Procedure](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/model-document-dp8-marketing-procedure-internal-only) for detailed information on sending marketing communications to individuals. In brief, you can send marketing information to individuals if:   1. You have their consent to send these communications; or 2. You can rely on the “soft opt-in” exception where you have had a previous commercial relationship i.e. sold them a service or product (which may not apply to work-seekers where you have only provided a work-finding service).   Other rules apply to marketing to organisations. |
|  | Consent | Consent is just one of six legal bases for processing personal data. To be valid, consent must be freely given, informed, specific and by affirmative action (i.e. not silence or pre-ticked boxes). Individuals can withdraw their consent at any time which would prevent the organisation further processing any data collected by consent. It will not always be appropriate to rely on consent and so organisations should consider if there is a more appropriate legal basis such as legitimate interests or performance of a contract.  For more detailed advice please see the [ICO guidance on consent.](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/)  If you wish to rely on consent use [Model Document DP6](https://www.rec.uk.com/recruiters/legal/template-documents/data-protection/model-document-dp6-consent-form) to obtain consent. |
|  | Legitimate interest | Where the processing of an individual’s personal data is based on a legitimate interest then the Company must set out the legitimate interests that they or a third party have pursued to process the data.  This can include for example:   * Managing your database and keeping work-seeker records up to date; * Contacting the individual to seek your consent where you need it; * Providing work-finding services to the individual. Please note that as per Regulation 19 of the Conduct Regulations neither an employment business nor an employment agency may introduce or supply a work-seeker to the client unless it has obtained confirmation (i.e. consent) that the work-seeker is willing to work in the position which the client seeks to fill; * Contacting the individual with information about similar products or services that they have used from you recently; and * Passing work-seeker’s information to debt collection agencies/other authorities.   Legitimate interest is quite broad and therefore flexible. However, this does not mean it should be used without proper consideration. Organisations that wish to use legitimate interests should carry out a legitimate interest impact assessment.  Please note that **legitimate interest cannot be used to process special categories of personal data**.  Please see the new [ICO guidance on legitimate interest](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/). Below is an extract from that guidance:  ***What is the ‘legitimate interest basis?***  *Article 6(1)(f) of the UK GDPR gives you a lawful basis for processing where:*  *“processing is necessary for the purposes of the legitimate interests pursued by the controller or by 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. “This can be broken down into a three-part test:*   1. ***Purpose test:*** *are you pursuing a legitimate interest?* 2. ***Necessity test:*** *is the processing necessary for that purpose?* 3. ***Balancing test:*** *do the individual’s interests override the legitimate interest?*   *A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.*  *‘Necessary’ means that the processing must be a targeted and proportionate way of achieving your purpose. You cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result.*  *You must balance your interests against the individual’s interests. In particular, if they would not reasonably expect you to use data in that way, or it would cause them unwarranted harm, their interests are likely to override yours. However, your interests do not always have to align with the individual’s interests. If there is a conflict, your interests can still prevail as long as there is a clear justification for the impact on the individual.* |
|  | Statutory/ contractual requirement | You need to inform the individual if the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter a contract. Recruitment businesses must collect certain personal data to meet statutory obligations, such as the Conduct of Employment Agencies and Employment Businesses Regulations 2003 – for example, they have to check identity, right to work, suitability for the role, qualifications and experience.  You will also need to inform the individual whether they are obliged to provide the personal data and the possible consequences of failure to provide such data. In reality, if a recruitment business does not or cannot do all of these checks it may not be able to introduce or supply a work seeker to a client. |
|  | Recipient of data | Where you have processed the individual’s data with a third party you will be obliged to inform the individual who such recipients or categories of recipients of that data are.  These can include for example:   * Clients that you introduce or supply individuals to (if you supply into a particular sector, you can choose give examples e.g. schools, nurseries, hospitals, care homes, local authorities, warehouses. You do **not** need to name each individual client; * Candidates’ former or prospective new employers that you obtain or provide references to; * The Recruitment and Employment Confederation (and any other trade body that you are a member of who may have access to your candidates’ data); * Any other third parties who carry out audits to ensure that you run your business correctly; * Payroll service providers who manage your payroll on your behalf; * Any umbrella companies that you pass candidate data to; * Other recruitment agencies in the supply chain (e.g. master/neutral vendors and second tier suppliers); * Your insurers; * Your legal advisers; * Social networks; * Your IT and CRM providers; * Any public information sources and third party organisations that you may use to carry out suitability checks on work-seekers e.g. Companies House, the Disclosure and Barring Service (DBS), Teaching Regulation Authority (TRA), Nursing and Midwifery Council (NMC), General Medical Council (GMC), DVLA, credit reference agencies etc.; * Government, law enforcement agencies and other regulators e.g. the Police, Home Office, HMRC, Employment Agencies Standards Inspectorate (EASI), Local Authority Designated Officers (LADOs), GLAA; * Trade unions; * Any of your group companies; and * Any other organisations an individual asks you to share their data with. Please note that this is not an exhaustive list. You will need to examine your recruitment practices and identify any parties that you process personal data with. |
|  | Section 2 - Categories and sources of data | Where you collect data from the individual directly you must give them the privacy notice at the time you collect the data.  Section 2 - If you collect data from other sources, you must give the individual information on both the categories and the sources of personal data you hold. You must do this within one month of collecting the data, or when you first communicate with the data subject if that is before one month expires. If you disclose the personal data to a third party and that disclosure happens before the one month expires, then you must give the transparency information no later than the first disclosure.  You can include the information set out in section 2 in your privacy statement to all if you wish (and if it is easier) but you must make sure to keep the individual informed if and when you collect other data from other sources. |
|  | Use of jobs boards and LinkedIn | Please see the [ICO Guidance on legitimate interest](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/) for an explanation of how recruiters can legitimately continue to use jobs boards and networking sites such as LinkedIn. |
|  | Overseas transfers | The UK GDPR **only** allows the transfer of personal data to countries outside of the UK in specific circumstances:     * Where an adequacy decision has been made in respect of the destination country; * Where the transfer is subject to appropriate safeguards; * Where the transfer is between members of a group of undertakings or enterprises that have adopted brining corporate rules; or * In one of the specific situations where a derogation applies.   If you are receiving personal data from a country, territory or sector covered by a European Commission adequacy decision (see below), the sender of the data will need to consider how to comply with its local laws on international transfers. Check local legislation and guidance and seek legal advice if necessary.  You don’t need any new arrangements for transfers from the UK to the EEA. The European Commission decides that a country can ensure an ‘adequate level of protection’ of *personal data*. A list of the third countries and territories/international organisations to which the European Commission has decided has an adequate level of protection is available on the [European Commission’s website.](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en) The countries currently listed include Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea Switzerland, the UK and Uruguay.  With regards to transfers subject to appropriate safeguards the UK GDPR provides for the following to enable data controllers and data processors to transfer personal data out of the UK:   * A legally binding and enforceable instrument between public authorities or bodies; * Binding corporate rules * Standard data protection clauses specified in regulations made by the Secretary of State under the Data Protection Act 2018 (DPA); * Standard data protection clauses specified in a document issued (and not withdrawn) by the ICO under the DPA 2018; * An approved code of conduct, together with binding and enforceable commitments of the controller or processor located in the third country to apply the appropriate safeguards, including as regards data subjects’ rights; and * An approved certification, together with binding and enforceable commitments of the controller or processor located in the third country to apply the appropriate safeguards, including as regards data subjects’ rights; as well as * Contractual clauses between the data controller or data processor and the data controller, data processor or recipient of personal data in a third country or an international organisation; or * Provisions to be inserted into administrative arrangements between public authorities or bodies (such as memoranda of understanding) which include enforceable and effective data subjects’ rights. |
|  | Data retention | You must set out how long you will store personal data for, or if that is not possible, how you decide how long to store the data.  As a recruitment business you must keep specific data for certain time periods for the purposes of the Conduct Regulations and tax legislation etc. If you process data for specified periods not already listed in this section then add this here.  The REC has produced [a record keeping table](https://www.rec.uk.com/legal-resources/legal-guide/gdpr/Record-keeping-table-2018-official.pdf) that you may find useful in helping you determine how long you intend to retain data.  Please note that the REC Legal team will not produce a retention policy for members. You will need to determine your own retention policy based on your business needs and any specific sector requirements. |
|  | Data retention – “do not supply lists” | Recruiters sometimes keep lists of work seekers they no longer wish to supply or introduce to clients i.e. a “do not supply list”. The UK GDPR does not expressly prevent keeping such a list but recruiters must have a legal basis for processing the data on that list (be aware though that there may be other reasons for not keeping a list such as potentially breaching the Equality Act 2010 if individuals with protected characteristics or members of Trade Unions are included on the list for no reason other than those protected characteristic). For example, the recruitment business will have a legitimate interest in recording safeguarding issues (there would also be a public interest in that) but this is quite different to recording someone’s state of dress which someone objected to or the fact that a client merely did not like them. If allegations were ever made against an individual were those allegations properly investigated prior to their inclusion on such a list?  If the recruitment business receives a subject access request, it would have to reveal if an individual was on a “do not supply list”. So, be careful about who and what is put on those lists and why – you must be able to justify keeping such a list and justify an individual’s inclusion on that list. |
|  | Your rights | You must tell the individual of their rights under current data protection laws, as well as their right to withdraw their consent to processing their personal data at any time. |
|  | Automated decision-making | An individual will have the right to know of the existence of any automated decision-making processes, including profiling, which produces legal effects on him or her or similarly significantly affects him on her.  If you have subjected the individual to automated decision making or profiling, then you will need to provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.  If you have not subjected the individual to automated decision making or profiling, you can either delete this section or include a statement to confirm that you do not use automated decision making.  REC Legal cannot advise you whether any particular software or process that you use is automated decision making or profiling. Please speak with your IT team or software provider for more information. |
|  | Cookies | Although there are different types of cookie, the Information Commissioner defines a cookie as ‘a small file, typically of letters and numbers, downloaded on to a device when the user accesses certain websites. Cookies are then sent back to originating websites on each subsequent visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site’.  The Privacy and Electronic Communications Regulations 2003 were implemented as a result of the Directive 2002/58/EC which sets out the rights of EU citizens when using electronic communications. The 2002 Directive was amended in 2009 and Article 5(3) now states that you must provide clear and comprehensive information about any cookies you are using and you must also obtain consent to store a cookie on a user or subscriber’s device. This was implemented into UK law on 26 May 2012.  Employment businesses and agencies who use cookies should ensure that they provide their website users with comprehensive cookie information and obtain their consent before storing any cookies.   Further information can be found on the ICO [website](https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies). |
|  | Complaints | The Company must inform the individual of their right to raise a complaint with the relevant authority (which is the ICO in the UK). However, it is a good idea to ask individuals to make a complaint to the Company so that you can try to resolve the issue internally. |

## Annex A

1. **The lawfulness of *processing* conditions for *personal data* are:**
2. ***Consent:****the individual has given clear consent for you to process their personal data for a specific purpose.*
3. ***Contract:*** *the processing is necessary for the performance of a contract with the data subject or in order to take specific steps before entering into a contract.*
4. ***Legal obligation:*** *the processing is necessary for compliance with a legal obligation to which the data controller/data processor is subject to.*
5. ***Vital interests:*** *the processing is necessary to protect someone’s life.*
6. ***Public task:*** *the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official functions, and the task or function has a clear basis in law.*
7. ***Legitimate interests:*** *the processing is necessary for the legitimate interests pursued by the data controller or a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests.*
8. **The lawfulness of *processing* conditions for *special categories of personal data* are:**
9. The *data subject* has given explicit consent to the *processing* of the *special categories of personal data* for one or more specified purposes, except where the *data subject* is not permitted or able to give *consent*.
10. *Processing* is necessary for carrying out obligations and exercising specific rights of the *data controller* or of the *data subject* under employment, social security or social protection law, in so far as it is authorised by UK law or a collective agreement, provided for appropriate safeguards for the fundamental rights and interests of the *data subject*.
11. *Processing* is necessary to protect the vital interests of the *data subject* or another person where the *data subject* is physically or legally incapable of giving *consent*.
12. *Processing* is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the *personal data* are not disclosed outside that body without the consent of the *data subject*(s).
13. *Processing* relates to *personal data* which manifestly made public by the *data subject*.
14. *Processing* is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
15. *Processing* is necessary for reasons of substantial public interest on the basis of UK law which is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject domestic law.
16. *Processing* is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of UK law or a contract with a health professional and subject to relevant conditions and safeguards.
17. *Processing* is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices on the basis of UK law.
18. *Processing* is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the *data subject*.