



Recruitment Privacy Notice

What is the purpose of this document?

DPDgroup UK Ltd (DPD UK) is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you when you apply for a job within DPD UK. This includes information provided through SmartRecruiters online job site, via email, by post, in person at interviews and/or by any other method.

Your personal information will be processed in accordance with the General Data Protection Regulation (GDPR), Data Protection Act 2018 and applicable Data Protection Laws.

It applies to all future candidates who wish to work within DPD UK.

DPD UK is a "Data Controller" of your personal information. This means that we are responsible for deciding how we hold and use personal information about you.

We are required under Data Protection Laws to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contracts to provide services.

We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you so that you are aware of how and why we are using such information.

Data protection principles

We will comply with the Data Protection Laws. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Adequate, relevant and limited to the purposes we have told you about..
4. Kept accurate and up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely in line with current best practice.

The kind of information we hold about you

Personal data or personal information means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

In order to process your job application, we will collect, store and use the following categories of personal information about you:

- Personal contact details such as name, title, address, telephone numbers, and personal email addresses.

Version:	Final	Last updated:	October 2019	Owner:	IT Security
----------	-------	---------------	--------------	--------	-------------

- Date of birth.
- Gender.
- National Insurance number.
- LinkedIn profile.
- Current salary and package, salary expectations.
- Details of friends or family that work for DPD - to comply with our personnel and family at work policy.
- Occupational questions such as the ability to work nights, weekends, shifts, etc.
- Copy of driving license or driving license number, passport, birth certificate and proof of current address, such as bank statements and utility bills.
- Evidence of how you meet the requirements of the job, including CVs evidencing work and employment history.
- Evidence of your right to work in the UK and immigration status.
- CCTV footage and other information obtained through electronic means such as door access control records.

There are “special categories” of more sensitive personal data that we may collect which requires a higher level of protection.

We may collect, store and use the following “special categories” of more sensitive personal information:

- Diversity and equal opportunities monitoring information – this can include information about your race or ethnicity, religious beliefs, sexual orientation, disability, and other ‘special category data’.
- Information about any special requirements you may require for an interview. I.e. you may wish to disclose a particular health condition in order for DPD UK to ensure we provide appropriate assistance.
- Information about criminal convictions and offenses.
- If you contact us regarding your application, a record of that correspondence.
- Details of your use of our recruitment tools and services, such as your candidate profile and alerts for vacancies.
- The status of your application and updates on how it moves forward

How is your personal information collected?

We collect personal information about candidates through the application and recruitment process, either directly from candidates using our applicant tracking system (SmartRecruiters), 3rd party job boards that you have signed up to, referrals, recommendations or sometimes from employment agencies.

As part of the application process, you will have the option to apply with your LinkedIn profile. The information on your profile will form the content of your application with DPD UK.

When you submit an application, we will ask you if you wish to be added to the DPD UK talent pool for 12 months. If you consent, you will be contacted by the recruitment team if your experience and qualifications are suitable for alternative roles with us.

Version:	Final	Last updated:	October 2019	Owner:	IT Security
----------	-------	---------------	--------------	--------	-------------

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- To move your application forward.
- To check that you are the right candidate for the role.
- To get in contact with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- To send you notifications for vacancy roles or job alerts.
- Where we need to perform the contract we have entered into with you.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We require all of the categories of information in the list above (see 'The kind of information we hold about you').

The purpose or purposes for which we are processing or will process your personal information are primarily to allow us to progress your job application and to enable us to comply with legal obligations.

In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Liaising with referees provided by you in order to obtain a reference.
- Administering the recruitment process.
- Making decisions about your salary.
- Assessing your qualifications for a particular job or task.
- Making decisions about your engagement.
- Education, training and development requirements.
- Complying with health and safety obligations.
- To prevent fraud.

- To conduct data analytics studies to review our recruitment process.
- Equal opportunities monitoring.
- Staff surveys before employment as part of our Employee Engagement Programme to improve services to our staff.

Some of the above grounds for processing will overlap and there may be several grounds that justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to process your job application.

Change of purpose

We will only use your personal information for the purposes for which we collected it unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Your data subject rights will not be affected.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

“Special categories” of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information.

We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent and understanding.
- Where we need to carry out our legal obligations or exercise rights in connection with employment.
- Where it is needed in the public interest, such as for equal opportunities monitoring.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information about your physical or mental health, or disability status when necessary, to make reasonable adjustments for an interview / assessment stage.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Version:	Final	Last updated:	October 2019	Owner:	IT Security
----------	-------	---------------	--------------	--------	-------------

Do we need your consent?

We do not need your consent if we use special categories of your personal information to carry out our legal obligations or exercise specific rights in the field of employment law.

In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, and give you the option to not participate or opt-out of processing.

You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will hold information about criminal convictions no longer than is necessary. Once the retention period has elapsed, your DBS certificate information is either immediately returned to you or destroyed by secure means.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however, we will notify you in writing if this position changes.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

Version:	Final	Last updated:	October 2019	Owner:	IT Security
----------	-------	---------------	--------------	--------	-------------

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with Smart Recruiters and other third parties where required by law, where it is necessary to administer the recruitment process with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

“Third parties” include third-party service providers (including agencies, agency job boards, LinkedIn, SmartRecruiters, contractors and designated agents) and other entities within our group.

The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services, Employment Checking Companies and employee surveys.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies.

We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance or system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example, we may need to share your personal information with a regulator or to otherwise comply with the law.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from dpo@dpdgroup.co.uk.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements as necessary.

Details of retention periods for different aspects of your personal information are available in our retention policy which is available from the DPO (Data Protection Officer).

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current.

Please keep us informed if your personal information changes during your application.

Your rights in connection with personal information

Under certain circumstances, by law, you have the right to:

- Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to the processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example, if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

Version:	Final	Last updated:	October 2019	Owner:	IT Security
----------	-------	---------------	--------------	--------	-------------

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data or request that we transfer a copy of your personal information to another party, please contact the HR Department.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time.

To withdraw your application and associated consent, you may log onto your candidate portal via the SmartRecruiter website. Alternatively, send your request via email to dpo@dpdgroup.co.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis to do so.

Data protection officer

We have appointed a data protection officer to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO at dpo@dpdgroup.co.uk or DPO, DPD UK, Broadwell Rd, Oldbury B69 4DA.

You have the right to obtain further information and guidance at any time from the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. Their contact details are: ICO, Wycliff House, Water Ln, Wilmslow SK9 5AF - ico.org.uk

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. Where necessary, we may also notify you in other ways from time to time about the processing of your personal information.

Version:	Final	Last updated:	October 2019	Owner:	IT Security
----------	-------	---------------	--------------	--------	-------------