

DRAX GROUP OF COMPANIES

JOB APPLICANT PRIVACY NOTICE

WHAT IS THE PURPOSE OF THIS DOCUMENT?

This Privacy Notice (“**Notice**”) is intended to provide information regarding how any personal information we collect from you or from third parties about you during and after the job application process. It relates to personal data, special category personal data or criminal convictions data (defined under data protection law) about you that we refer to as personal information in this Notice.

WHO COLLECTS THE INFORMATION

Drax Group companies, including Drax Power Limited, Drax Generation Enterprise Limited, SMW Limited, Haven Power Limited and Opus Energy Limited (“**Company**”, “**we**”, “**us**”, or “**our**”), are the joint data controllers of personal information provided by you or collected about you. This means that we are responsible for deciding how we hold and use personal information about you and that we are required to notify you of the information contained in this Notice. It is important that you read this Notice so that you are aware of how and why we are using your personal information and how we will treat it. Depending on the circumstances, we may on occasion provide you with a shorter privacy notice to cover specific types of processing that will be supplemented by this Notice.

This Notice applies to current and former applicants for job roles. This Notice does not form part of any future contract of employment or other contract to provide services. We may update this Notice at any time, so you are advised to review this Notice at regular intervals.

Please read this Notice as if its from your potential employing Company. However, your personal information will also be shared within our Drax group of companies (our “**Drax group companies**”) and so, in this Notice, references to ‘we’ or ‘us’ mean the Company and our Drax group companies.

We respect your privacy and are committed to protecting your personal information. Our Group Data Protection Officer is responsible for overseeing questions in relation to this Notice. If you have any questions about this Notice, please use the contact details set out at the end of this Notice in the “Contacting Us” section.

DATA PROTECTION PRINCIPLES

We will comply with data protection law.

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. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

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:

- Where we need to enter into a contract of employment with you or where we need to perform under an employment contract with you*;
- Where we need to comply with a legal obligation, for example, to ensure we make any reasonable adjustments under disability law**;
- Where you give us consent, for example, when we are collecting diversity data***; and/or
- 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, for example, carrying out surveys about applicant experience****.

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

- Where we need to protect your vital interests (or someone else's interests), for example, if you are involved in a serious accident and we need to provide health information to the accident responders;
- Where it is needed in the public interest or for official purposes, for example where we carry out equalities monitoring.

Situations in which we will use your personal information

The situations in which we will process your personal information are listed below. We have indicated by asterisks the purpose or purposes for which we are processing or will process your personal information, as well as indicating which categories of personal information are involved.

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

THE KIND OF INFORMATION WE COLLECT

To decide whether to shortlist you as an applicant and to contact you in relation to your application*/**, we will need to collect the following information about you up to and including the shortlisting stage of the recruitment process:

- Your name and contact details (e.g. address, home and mobile phone numbers, email address);
- Your curriculum vitae/resume;
- Details of your qualifications, experience, employment history (including job titles and salary);
- Whether you have worked on Smart Systems as part of your employment (where applicable); and
- Your eligibility to work in the United Kingdom.

We will not be able to process your application without this information.

If we decide to invite you to attend an interview, in certain circumstances we may need to collect the following personal information about you (you will be notified in advance):

- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information**;
- Copies of documents containing your name, address and date of birth to enable us to verify your identity*;
- A copy of your driving licence*/** if relevant for your role.

After we have made a conditional job offer, we will need to collect the following personal information about you to allow us to make our final decision as to whether to recruit you*/**:

- Information about your previous academic and/or employment history from references obtained about you from previous employers and/or education providers;

- Information regarding your academic and (where relevant) professional qualifications; and
- Information regarding your unspent criminal convictions obtained through a DBS Basic Check, if required for your role.

Dependant upon your job role, we are under a statutory obligation to collect information from you regarding your criminal record, your nationality and immigration status and information from related documents, and a copy of your driving licence to enable us to verify your right to work in the United Kingdom**.

If your application is successful, we will use the information provided above to the extent necessary to administer your employment*. Further details about how we will process your personal information pursuant to your employment will be provided in our Employee Privacy Policy.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We will collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies. If we do so, you will be provided with more specific information at the time.

POINTS TO NOTE

Your personal contact details will be stored in case of emergency. Such emergencies include but are not limited to notifying you that the location of the planned interview or testing is not accessible, for example, due to bad weather and advising you that due to an incident, normal operations are suspended or being managed elsewhere***.

If you do not provide personal information

If you do not provide certain information when requested we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers or to verify your right to work in the UK).

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.

HOW WE USE SENSITIVE PERSONAL INFORMATION

You may volunteer and we may also receive from you information that we could store and use. The following “special categories” of more sensitive personal information if it relates to your potential employment with us:

- Information about your health, including any medical condition, health and sickness records;
- Information about your race or ethnicity, religious beliefs or sexual orientation;
- Trade union membership, where appropriate;
- Information about criminal convictions and offences.

“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 may process special categories of personal information in the following circumstances:

- Where we need to carry out our legal obligations, for example, complying with health and safety obligations and in line with our Privacy Policy;

- Where it is needed in the public interest, for example, equal opportunities monitoring and in line with our Privacy Policy;
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards;
- In limited circumstances, with your explicit written consent.

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 a potential employer

We may use personal data about your physical or mental health, or disability status, to ensure your health and safety on our site and to provide appropriate adjustments.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy (our Privacy Policy) 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 personal information, for example ethnicity. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your employment contract with us that you agree to any request for consent from us.

INFORMATION ABOUT CRIMINAL CONVICTIONS

Where we are legally permitted and/or required, and it is appropriate given the nature of your role (e.g. a finance role, where you are going to be working at one of our visitor centres or on Smart Systems), we may collect information about unspent criminal convictions as part of the recruitment process and we may repeat those checks from time to time during your employment with us as considered necessary.

We will use information about unspent criminal convictions to meet our legal obligations such as to assess whether your continued employment poses an unacceptable risk to us, our customers or our employees / workers.

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 our employment 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.

As a part of your candidate experience we ensure that all applications made to us are reviewed by a member of our recruitment team. We confirm that will not make any decisions about you using automated means, however we will notify you in writing if this position changes.

DATA SHARING

We may have to share your personal information with third parties, including third-party service providers and other companies in the Drax group. We require third parties to respect the security of your personal information and to treat it in accordance with the law. We have a Third-Party Onboarding Privacy Policy that governs our appointment of third-party service providers where we may share, or they may be able to access, personal information that we control. It requires us to carry out due diligence on them and to ensure appropriate data protection terms are in our agreement with them.

Why might we share your personal information with third parties?

Where we use video conferencing and other technology facilities to conduct an interview with you, we are required through a third party system to share your personal information to facilitate the call.

Which third-party service providers process my personal information?

“Third parties” includes third-party service providers (including contractors and designated agents) and other entities within our Drax group of companies.

When might we share your personal information with other Drax group companies?

We will share your personal information with other companies in the Drax group as part of our regular human resources processes and for system maintenance support and hosting of personal information.

Transferring information outside the United Kingdom (UK) European Union (EU)

Most of the personal information we collect about you is based in the United Kingdom or in some cases, a service provider or their sub-processor may be based outside the UK or the EU and so, they are required to comply with UK or European data protection law. On occasion, we may appoint a third-party service provider whose operation or a server or sub-processor may be based outside of the UK or EU. As part of our Third-Party Onboarding Privacy Policy, we carry out due diligence on our third-party providers and assess whether your personal information will be transferred to them or accessed by them from outside the UK or EU. If that is the case, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- we will only transfer your personal information to countries that have been deemed to provide an adequate level of protection for personal information by the European Commission¹; or
- where we use providers based in the US, we may transfer personal information to them if they are part of the Privacy Shield which requires them to provide similar protection to personal information shared between the UK and the US. You can view certifications at www.privacyshield.gov²; or
- where we use certain service providers who are not in a ‘adequate’ country or part of the Privacy Shield, we may use specific contracts approved by the European Commission which give personal information the same protection it has in the UK and EU, called an EU Model Clause Agreement³.

¹ Article 45 of the GDPR

² Article 46 of the GDPR

³ Article 46 of the GDPR

If you would like to know the specific mechanism used by us when transferring your personal information out of the UK or EU, please contact us using the details in the “Contacting Us” section at the end of this Notice.

DATA SECURITY

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 such as corporate firewalls protecting multi-layer server configuration and penetration testing. If you would like to know more, contact us using the details in the “Contacting Us” section at the end of this Notice.

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 and an obligation to comply with data protection law. See the Data Sharing section above for further information.

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

DATA RETENTION

How long will we use your information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

Personal information relating to unsuccessful applicants will be deleted or anonymised at the latest 12 months following the last time you logged into our recruitment system, unless you have agreed to us retaining your details so that we can inform you of any suitable vacancies that arise, in which case we will retain your personal information for up to 2 years.

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 responsibility 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 working relationship with us by logging into your account and updating the information.

Your rights in connection with personal information

Data protection laws provide you with the following rights:

- **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. It is possible for you to update your information within our recruitment system yourself;
- **Request erasure** of your personal information in certain circumstances. 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). However, this is not an absolute right and there will be circumstances where we are required to retain your personal information even if you are no-longer an employee of ours, for example, to defend a legal claim. It is possible for you to update your information within our recruitment system yourself ;
- **Request the restriction of processing** of your personal information in certain circumstances. 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;
- **Request the transfer** of your personal information to another party.

You also have a **Right to 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.

If you want to exercise any of these rights, please contact us using the details in the “Contacting Us” section at the end of this Notice.

Please note, you have the right to make a complaint at any time to the UK regulator for data protection issues, the Information Commissioner’s Office (ICO). The ICO can be contacted by telephone on 0303 123 1113 or by post at Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or via email at casework@ico.org.uk. We would, however, appreciate the chance to deal with your concerns before you approach the ICO, so please contact us in the first instance using the contact details set out below.

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.

Timing of our response

We do our best to respond to all legitimate requests within one calendar month. Occasionally, it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

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 consent, please contact us using the details in the “Contacting Us” section at the end of this Notice. 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 for doing so in law.

CHANGES TO THIS PRIVACY NOTICE

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

DATA PROTECTION OFFICER AND CONTACTING US

Our Group Data Protection Officer (GDPO) oversees compliance with this Notice.

If you have any queries, comments or requests regarding this Notice or you would like to exercise any of your rights set out above, you can contact us as follows:

Generation and Core Services job applicants (shown as Drax Group and Drax Power on our job applicant website)

- by post to our GDPO at Drax Power Limited, Drax Power Station, Selby, North Yorkshire, YO8 8PH; or
- by email to our GDPO at data.protection@drax.com

Haven Power job applicants

- by post to our Data Protection Practitioner, Haven Power Limited, 32 The Havens, Ransomes Europark, Ipswich, IP3 9SJH; or
- by email to our Data Protection Practitioner at data.protection@havenpower.com

Opus Energy applicants

- by post to our Data Protection Practitioner, Opus Energy Limited, Opus Energy House, The Lakes, Northampton, NN4 7YD; or
- by email to our Data Protection Practitioner at data.protection@opusenergy.com