

CCTV Privacy Notice



drax

CCTV Privacy Notice

WHAT'S THE PURPOSE OF THIS DOCUMENT?

As we are committed to the safety of our staff and visitors we use a closed-circuit television system ("CCTV") at our sites. The purpose of this document is to set out how the CCTV system will be managed and used by the Company and to inform individuals, whose personal data may be captured on the CCTV system, about how and why that personal data may be processed by the Company.

WHO COLLECTS THE INFORMATION?

Drax group companies, including Drax Corporate Limited, Drax Power Limited, Drax Generation Enterprise Limited, SMW Limited, Haven Power Limited and Opus Energy Limited ("Company", "we", "us", or "our"), are the data controllers of personal information 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.

COMPLIANCE

The Company is aware that images of recognisable individuals, such as staff and site visitors, captured by the CCTV system constitute 'personal data', use of which is governed by data protection law.

The Company will ensure that its use of the CCTV system and the personal data that it captures complies with the law.

This document has been drafted in accordance with the Information Commissioner's Office (ICO) CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice. Copies of these codes can be found at www.ico.org.uk and <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice> respectively.

PURPOSE OF THE CCTV SYSTEM

The purpose of the CCTV system is:

- To increase the personal safety of our staff and visitors to our sites;
- To support our health and safety measures;
- To assist in identifying, apprehending and prosecuting any offenders on Company sites;
- To protect the Company's buildings and assets and those of its staff from intrusion, theft, vandalism, damage or disruption.

The legal basis for the Company's use of any personal data which is captured by the CCTV system is that the processing is necessary for the legitimate interests set out in this paragraph (provided that those interests are not overridden by individuals' rights and interests). The Company may also need to use this personal data in order to establish, exercise or defend against legal claims.

OPERATION

CCTV cameras are located at strategic points on our sites, primarily access points, such as the gates to the sites, in office areas and in certain production areas. Signs are displayed prominently around the sites to inform staff and visitors that CCTV cameras are in operation and who to contact for further information.

The cameras are in operation 24 hours a day, 7 days a week and they will be monitored from the Security Control Room based at the Drax Power Station near Selby in the UK. Drax Power Limited is a company in the Company's group of companies and manages all the footage from the CCTV cameras. In addition, the cameras can be monitored by Company security staff at the relevant Company site. We also use a third party provider who will regularly check and confirm the efficiency of the system, including that the equipment is properly recording, that the cameras are functional, that the time and date are correct and that that footage is being deleted or retained in accordance with this document.

The CCTV system is regularly maintained in accordance with the manufacturer's instructions.

SECURITY

Physical protective measures: The Security Control Room can only be accessed with the correct access control privilege, which is primarily limited to security staff. A record is kept of all those who are given access to the Control Room.

Technical protective measures: We have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. This includes ensuring CCTV hard drives are located in a secured server room and access to this room is only via a formal approval process. Password protection, technical access control and the use of encryption are also technical protection measures that we use.

We have put in place procedures to deal with any suspected personal data breach and will notify any affected individuals and/or the ICO where appropriate.

ACCESS AND DISCLOSURE

Access to recorded CCTV footage is restricted to a limited number of security staff as authorised by the Security Operations Manager from time to time ("Authorised Persons") and all requests for disclosure of CCTV footage must be submitted to one of these Authorised Persons.

CCTV footage may only be accessed or disclosed to the extent necessary in order to deal with an incident which falls within the purpose identified above or in order to respond to a request made by an individual under the law (see further below). CCTV footage will not be accessed or used for any other purpose.

CCTV footage will be viewed in a secure office and any access to and any disclosures of recorded footage will be recorded in the CCTV log. This process is overseen by the Security Operations Manager and as appropriate, with reference to the relevant member of our Data Protection team.

External disclosure of CCTV footage will usually not be permitted other than to law enforcement agencies or to regulators, or in order to comply with a court order. CCTV footage will not be uploaded to the internet.

TRAINING

All staff who may be involved in the management or operation of the CCTV system will be trained in how to comply with this document and to ensure that the system is used in accordance with the law.

COVERT RECORDING

Covert recording will only be carried out in very limited circumstances and with the authorisation of our Head of Security and/or Group Data Protection Officer.

Covert surveillance will only be carried out where specific criminal activity is suspected and where informing the relevant individuals would be likely to prejudice the prevention of crime and/or apprehension/prosecution of the offender.

Any authorisation to use covert recording will be documented in writing and include confirmation that it is required to obtain evidence of suspected criminal activity in a specific case, an assessment of the alternative methods of obtaining the evidence and the permitted duration of the covert recording. The authorisation will be regularly reviewed, for example, every 28 days, to assess whether it is continued to be required or should cease.

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 usually notify you and we will explain the legal basis which allows us to do so.

DISCLOSURE OF YOUR INFORMATION

We may share your personal information with the third parties set out below for the purposes described above:

- service providers (generally based in the UK) such as those who provide IT and system administration services
- other companies in our Group of companies who provide security, IT and system administration services and undertake management reporting and statistical analysis to improve our product and service offering
- if we are under a duty to disclose or share your personal information in order to comply with any legal obligation, or in order to enforce or apply our contract with you
- in the event that we sell or buy any business or assets, in which case we may (where relevant) disclose your personal information to the prospective seller or buyer
- if we, or substantially all of our assets, are acquired by a third party, in which case personal information held by us will be one of the transferred assets
- to protect the rights, property or safety of us, our customers and others. This includes exchanging information with other

organisations such as fraud and theft prevention agencies for the purposes of reducing credit risk, fraud and energy theft.

We require all service providers and Group companies that we share your personal information with to respect the privacy and security of your personal information and to treat it in accordance with the law. We do not allow our third-party service providers, including Group companies, to use your personal information for their own purposes and only permit them to process your personal information for specified purposes and in accordance with our instructions.

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 in the European Union (EU) and so, they are required to comply with 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 EU. As part of our Third Party Privacy Onboarding 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 EU. If that is the case, we ensure a similar degree of protection is afforded to it. If you would like to know the specific mechanism used by us when transferring your personal information out of the EU, please contact us using the details set out in the "Contacting Us" section at the end of this Notice.

INFORMATION RETENTION

The images captured by the CCTV System will not be stored for any longer than is required in order to achieve the purposes identified above. CCTV footage will automatically be deleted on a 30-day rolling basis, unless specific images are required in order to deal with an incident or in order to respond to a request by an individual made under the law (see further below).

YOUR RIGHTS

Data protection laws provide you with the following rights where we are processing your personal information 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);
- 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; and
- request a copy of your personal information which you

have provided to us, in a structured, commonly used and machine-readable format and the right to transfer it, or to require us to transfer it directly, to another controller.

You also have the “**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. You also have the right to object where we are processing your personal information for direct marketing purposes.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights above). 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.

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.

You have the right to make a complaint at any time to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues. The ICO can be contacted by telephone on 0303 123 1113 or by post as follows: 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 any of the details set out below in the “Contacting Us” section.

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.

CONTACTING US

If you wish to make an individual rights request, or you are a law enforcement or government organisation wishing to make an enquiry, please visit our [secure portal](#).

Any queries or complaints about the CCTV system should be addressed to the Security Operations Manager at Drax Power Station, Selby, North Yorkshire, YO8 8PH or via email to securityoperationsmanager@drax.com.

Updated: September 2020