BORD NA MÓNA
Naturally Driven

AES
Data Protection
Privacy Policy

Contents

Purpose

Bord na Móna Plc, its subsidiaries and their subsidiaries (for the avoidance of doubt Advanced Environmental Solutions (Ireland) Limited **(AES))** ("**we**" or "**AES**") collects, uses, shares and holds certain Personal Data about current, past and prospective consumers, customers, suppliers, business contacts, employees and other people in course of its business activities. Personal Data must be Processed in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") and other applicable national and European privacy legislation and regulations (together the "**Data Protection Law**").

AES recognises the need to treat Personal Data in an appropriate and lawful manner and is committed to complying with its obligations in this regard. This Privacy Policy explains how we use Personal Data.

This Privacy Policy applies to all entities within the Bord na Móna group and all individual who work for, with or on behalf of any Bord na Móna business including AES.
We use the words Personal Data to describe information that is about you or others from which you or they are identifiable. Other key data protection terms are defined in Schedule 1 *(Definitions of key data protection terms)*.
The purpose of this Privacy Policy is to:

a) ensure AES protects the right of customers, staff and partners;

b) describe what personal data AES holds and how it processes it;

c) ensure AES complies with the Data Protection Law; and

d) allow AES to demonstrate compliance with the Data Protection Law with particularly in accordance with Article 24(1) of the GDPR.

This Privacy Policy may be supplemented by other privacy notices tailored to our specific relationships with you.
If you have any questions in relation to this Privacy Policy, your rights in relation to your personal data or any other queries please contact the Data Protection Officer ("**DPO**") at informationofficer@bnm.ie.

This policy is part of the appropriate arrangements and structures put in place that are, in the Directors' opinion, designed to secure material compliance with the company's "relevant obligations" under the Companies Act 2014.

Personal Data we process

AES holds personal data in relation to current, past and prospective:

a) customers;

b) employees;

c) suppliers; and

d) business contacts.

A person whose personal data we hold hereafter referred to as "you" and "your" shall have a corresponding meaning.

.

Personal Data we may hold and process is further described in Schedule 2 *(Types of Personal Data)*. We endeavour to keep the Personal Data we Process accurate and up to date and held securely.

How we use Personal Data

We use Personal Data to carry out our business activities. The purposes for which we use your Personal Data may differ based on our relationship, including the type of communications between us and the services we provide.

The main purposes include using Personal Data to:

- provide our products and services;
- manage the employment relationship including to process payroll for our employees, make corporate discounts available to our employees, distribute the company magazine to our employees;
- process customer and supplier invoices;
- communicate with you and other individuals;
- improve the quality of our products and services, provide training and maintain information security [(for example, for this purpose we may record or monitor phone calls to improve our quality of service to our customers.)];
- carry out research and analysis, including analysis of our customer base and other individuals whose Personal Data we collect;
- provide marketing information in accordance with preferences you have told us about (marketing information may be about offers or discounts or our other products and services);
- manage our business operations and IT infrastructure, in line with our internal policies and procedures;
- manage complaints, feedback and queries, and handle requests for data access or correction, or the exercise of other rights relating to Personal Data;
- comply with applicable laws and regulatory obligations, for example, laws and regulations and statutory responsibilities relating to employee working time regulations tax, national insurance, statutory sick pay, statutory maternity pay, family leave, work permits, equal opportunities monitoring, anti-money laundering, sanctions and anti-terrorism; comply with legal process and court orders; and respond to requests from public and government authorities (including those outside your country of residence); and
- establish and defend legal rights to protect our business operations, and those of our business partners.

Automated decisions using Personal Data

We may use automated decision making tools (i.e. where a person is not involved in the decision).We typically use these tools when making straightforward decisions about you. Where this is the case we may provide you with more information at the time to aid your understanding of what is involved.

Responsibility for Personal Data

AES is responsible for looking after your Personal Data in accordance with this Privacy Policy, our internal standards and procedures, and the requirements of data protection law.
When employees or others that work on AES's behalf handle Personal Data we will always ask that they treat Personal Data in a confidential and secure manner and will require them to comply with the Confidentiality Code of Conduct set out in Schedule 3.

Sharing of Personal Data

In connection with the purposes described above, we may need to share your Personal Data with third parties. The types of third parties with which we may share your Personal Data are further described in Schedule 3 *(Third Party Disclosures)*.

When we provide Personal Data to third parties, the third parties will be selected carefully and required to use appropriate measures to protect the confidentiality and security of the Personal Data. Those third parties will assume certain responsibilities under the Data Protection Law for looking after the Personal Data that they receive from us.

In certain circumstances, Data Protection Law allows Personal Data to be disclosed to law enforcement agencies without the consent of the Data Subject. In such circumstances, we will disclose requested Personal Data to the extent permitted by, and in accordance with, applicable Data Protection Law.

International Transfers of Personal Data

For the purposes set out in this Privacy Policy we may transfer Personal Data to parties located in other countries that have data protection regimes which are different to those in Ireland and which have not been found by the European Commission to provide adequate protection for Personal Data.

When making these transfers, we will take steps to ensure that your Personal Data is adequately protected and transferred in accordance with the requirements of the Data Protection Law.

This may involve the use of data transfer agreements in the form approved by the European Commission or another mechanism recognised by data protection law as ensuring an adequate level of protection for Personal Data transferred outside the EEA (for example, standard contractual clauses).

For further information about these transfers and to request details of the safeguards in place, please contact by email at: informationofficer@bnm.ie.

Security of Personal Data

AES uses appropriate technical, physical, legal and organisational measures, which comply with data protection laws to keep Personal Data secure.

As most of the Personal Data we hold is stored electronically we have implemented appropriate IT security measures to ensure this Personal Data is kept secure. For example, we may use anti-virus protection systems, firewalls, and data encryption technologies. We have procedures in place at our premises to keep any hard copy records physically secure. We also train our staff regularly on data protection and information security. It is the responsibility of all employees to handle Personal Data securely and in line with such data security and storage guidelines set out by the company from time to time.

When AES provides Personal Data to a third party (including our service providers) or engages a third party to collect Personal Data on our behalf, the third party will be selected carefully and required to use appropriate security measures to protect the confidentiality and security of Personal Data. For example Personal Data is encrypted / password protected where appropriate.

Unfortunately, no data transmission over the Internet or electronic data storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any Personal Data you might have sent to us has been compromised), please immediately notify us.

Data Breach

If there is ever a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, AES will follow the AES Data Breach Procedure.

Legal justifications for our processing of Personal Data

To comply with Data Protection Law, we need to tell you the legal justification we rely on for using your Personal Data for our purposes.
While the law provides several legal justifications, the table in Schedule 4 *(Legal Basis for Processing)* describes the main legal justifications that apply to our purposes for using Personal Data.
Where we rely on our legitimate business interests or the legitimate interests of a third party to justify the purposes for using your Personal Data, our legitimate interests will usually be:

- pursuit of our commercial activities and objectives, or those of a third party (for example, by carrying out direct marketing);
- compliance with applicable legal and regulatory obligations, and any guidelines, standards and codes of conduct (for example, by carrying out background checks or otherwise preventing, detecting or investigating fraud or money laundering);
- improvement and development of our business operations and service offering, or those of a third party;

- protection of our business, shareholders, employees and customers, or those of a third party (for example, ensuring IT network and information security, enforcing claims, including debt collection); and
- analysing competition in the market for our services (for example, by carrying out research, including market research).

For Processing of more Sensitive Personal Data we will rely on either:

- your consent;
- that use of your Sensitive Personal Data is necessary for the purpose of the assessment of the working capacity of an employee and to enable AES to provide suitable accommodations where necessary; or
- that use of your Sensitive Personal Data is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity (for example, when a court issues a court order requiring the Processing of Personal Data).

Monitoring

We may record telephone calls with you so that we can:

- improve the standard of service that we provide by providing our employees with feedback and training;
- address queries, concerns or complaints;
- prevent, detect and investigate crime, including fraud and money laundering, and analyse and manage other commercial risks; and
- comply with our legal and regulatory obligations.

In addition, we monitor electronic communications between us (for example, emails) to protect you, our business and IT infrastructure, and third parties including by:

- identifying and dealing with inappropriate communications; and
- looking for and removing any viruses, or other malware, and resolving any other information security issues.

Our use of CCTV involves Processing of Personal Data. Further information on how we Process Personal Data using CCTV is set out in 0.

Retention of Personal Data

We will keep Personal Data for as long as is necessary for the purposes for which we collect it. Where we hold Personal Data to comply with a legal or regulatory obligation, we will keep the information for at least as long as is required to comply with that obligation. In some cases a retention period will apply once the initial purpose has ceased e.g. financial information is kept for 7 years, payroll files are required to be kept for current year plus 6 years.

Where we hold Personal Data in order to provide a product or service, we will keep the information for at least as long as we provide the product or service, and for a number of years thereafter. The number of years varies depending on the nature of the product or service provided.

AES endeavours to ensure that Personal Data will only be kept for a period which is relevant and not excessive to achieve the purposes for which it is being held. Personal Data will be deleted once that purpose is achieved or it is no longer required.

Your personal data rights

Schedule 6 sets out a summary of the data protection rights available to individuals in the EEA in connection with their Personal Data. These rights may only apply in certain circumstances and are subject to certain legal exemptions.

Any request to exercise your rights should be sent to the DPO at informationofficer@bnm.ie. To help us to respond to your request, please be as specific as possible. For example, if you wish to exercise your right to access your Personal Data, please specify the Personal Data of which you wish to obtain a copy.

Please include any additional details that would help us to respond to your request - for example, your customer account number, a staff reference number, names of departments/offices that you were associated with, etc.
If you wish a third party to submit a request to exercise your rights on your behalf (e.g. a family member or solicitor), you must provide written authorisation to allow us to disclose your Personal Data to that third party.

You may be asked to provide further information in order for AES to confirm your identity.

Who to contact about your Personal Data

If you have any questions or concerns about the way your Personal Data is used by us, you can contact us by email at: informationofficer@bnm.ie.

Review and Revision

We review this Privacy Policy regularly and reserve the right to make changes at any time to take account of changes in our business, legal requirements, and the manner in which we process Personal Data. This Privacy Policy was last updated on 22nd of May 2018. We may review this policy and make changes from time to time.

SCHEDULE 1

Definition of key data protection terms

"**Data Controller**" means the entity that controls Personal Data, by deciding why and how such Personal Data is Processed.

"**Data Processor**" means the party that Processes Personal Data on behalf of the Data Controller (for example, a payroll service provider).

"**European Economic Area**" or "**EEA**" means Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the UK, Iceland, Liechtenstein, and Norway.

"**Personal Data**" is any information relating to a living individual which allows the identification of that individual. Personal Data can include:

- a name,
- an identification number;
- details about an individual's location; or
- any other information that is specific to that individual.

"**Processing**" includes collecting, using, recording, organising, altering, disclosing, destroying or holding Personal Data in any way. Processing can be done either manually or by using automated systems such as information technology systems and "**Process**" and "**Processing**" shall be interpreted accordingly.

"**Profiling**" is the automated Processing of Personal Data for the purpose of assessing certain aspects relating to an individual so as to analyse or predict the individual's performance, decisions or behaviour.

"**Sensitive Personal Data**" are types of Personal Data that reveal any of the following information relating to an individual: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Special Categories of Personal Data also include the Processing of genetic data, biometric data (for example, fingerprints or facial images), health data, data concerning sex life or sexual orientation and any Personal Data relating to criminal convictions or offences.

SCHEDULE 2

Types of Personal Data

Type of Personal Data	Examples
Contact information	Name, address, email, telephone number and emergency contact details
General information	Gender, marital and family status, date and place of birth, and physical characteristics.
Education and prior employment	Educational background, employer details and employment history, skills and experience, professional licences, memberships and affiliations.
Government	Social security number, passport number, tax number, driver's licence number, or other government issued identification number.
Financial information	Payment card number (credit /debit card), bank account number, other financial account number and account details, other financial information.
HR information	Records of holiday, sickness and other absence; records relating to your career history such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records
Marketing preferences, marketing activities and customer feedback	Marketing preferences or responses to customer satisfaction surveys.
Online activity information	Any online interaction with our website presence is covered under our Website Privacy Policy. Please refer to our Corporate Website for more information or contact informationofficer@bnm.ie.
Supplemental information from other sources	We and our service providers may supplement the Personal Data we collect with information obtained from other sources (for example, third party commercial information sources, and information from our business partners).

SCHEDULE 3

Confidentiality Code of Conduct

AES employees and all others who work with or on behalf of AES must comply with this confidentiality code of conduct (the "**Code**"). AES *will ensure that all those subject to this policy are made aware of it at the outset of their work with the company*.

1. What is Confidential Information?

Confidential Information means all business, technical, financial, operational, administrative, marketing, economic and other information and material relating to AES's business, and all Personal Data of employees or customers of AES either in written, oral or any other form, to which you may have access.

2. Confidentiality and Non-Disclosure Requirements

Confidentiality is an intrinsic element to the work of AES. The importance of confidentiality must be clearly understood by all AES employees and all others who are or will be required to work with or on behalf of AES.

2.1 For the duration of employment with AES and at all times after the termination of employment with AES, employees must keep all Confidential Information secret and treat it as confidential and must not, without the prior written consent of AES (which may be given, if at all, on such terms as AES considers appropriate), be disclosed (whether in written, oral or in any other form) in whole or in part to any other person. Employees must not use the Confidential Information for any purpose other than in connection with their role as an employee of AES.

2.2 Employees cannot discuss any confidential information relating to AES (or related Companies or their businesses) or data in respect of which AES owes an obligation of confidence to any third party during or after their employment except in the proper course of their employment or as required by law.

2.3 Employees cannot remove or copy any document or things belonging to AES which contain any confidential information from AES's premises at any time without proper advance authorisation.

2.4 Employees must return to AES upon request and, in any event, upon the termination of their employment, all documents and things belonging to AES or which contain or refer to any Confidential Information and which are in your possession or under their control.

3. Maintaining Confidentiality

AES and all others who are or will be required to work on behalf of AES or with documentation and/or related systems have an obligation to ensure confidentiality and compliance with the Data Protection Law, Bord na Móna's IT security policies, which have been separately notified to employees, and the security measures outlined in the Data Security and Storage Guidelines must be adhered to.

Third Party Disclosures

Type of third party	Examples
Service providers	External third party service providers, such as security professionals, accountants, auditors, experts, lawyers and other professional advisors; travel assistance providers; call centre service providers; IT systems, support and hosting service providers; advertising, marketing and market research, and data analysis service providers; banks and financial institutions that service our accounts; document and records management providers; and other third party vendors and outsourced service providers that assist us in carrying out business activities.
Government / Judicial authorities	We may also share Personal Data with: (a) government or other public authorities (including, but not limited to, courts, regulatory bodies, law enforcement agencies, tax authorities and criminal investigations agencies); and (b) third party participants in legal proceedings and their accountants, auditors, lawyers, and other advisors and representatives, as we believe to be necessary or appropriate.

SCHEDULE 4

Legal Basis for Processing

Purpose of Processing	**Legal Justifications**			
	Consent	Contractual Necessity	Legal Requirement	Legitimate Interests
To communicate with you		●	●	●
For the employment relationship		●	●	●
To provide products and services		●		●
To invoice customers and suppliers		●		
To improve the quality of our products and services, for training, and to maintain information security			●	●
To manage commercial risks			●	●
To carry out research and analysis	●			●
To provide marketing information and promotions	●			●
To manage our business operations and IT infrastructure		●	●	●
To manage complaints, feedback and queries		●	●	●
To comply with applicable laws and regulations			●	●

SCHEDULE 5

CCTV Policy

1. Introduction

Closed circuit television systems ("CCTV") are installed in all premises under the control of Bord na Móna Plc, its subsidiaries and their subsidiaries (for the avoidance of doubt Advanced Environmental Solutions (Ireland) Limited (AES)) (the "Company").

2. Purpose of Policy

The purpose of this Policy is to regulate the use of CCTV and its associated technology in the monitoring of both the internal and external environs of all premises operated by the Company in Ireland.

CCTV systems are installed both internally and externally in premises for the purpose of enhancing security of Company premises and associated equipment, as well as creating awareness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day.

CCTV surveillance at Company premises is intended for the purposes of:
protecting Company buildings and assets, both during and after hours; and
promoting the health and safety of staff and visitors.

3. Scope

This Policy applies to all Company personnel and visitors and relates directly to the location and use of CCTV and to the monitoring, recording and subsequent use of material recorded by CCTV.

4. General principles

The Company has a responsibility for the protection of its property, equipment and resources as well providing a sense of security to its employees and visitors to its premises. The Company owes certain duties under the provisions of health and welfare at work legislation and utilises CCTV as an added mode of security.

The use of CCTV will be conducted in a professional, ethical and legal manner.

Use of CCTV is required to be compliant with this Policy following its adoption by the Company. Recognisable images captured by CCTV are subject to the provisions of the General Data Protection Regulation (EU 2016/679) and the [Data Protection Act 2018] (the "Data Protection Law") to the extent they are personal data. "Personal data" mean data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller, with the Company being the data controller.

5. Use of CCTV footage

Information obtained through CCTV may only be released when authorised by the Data Protection Officer ("DPO").

Any requests for record CCTV images by An Garda Síochána will be fully recorded and legal advice will be sought if any such request is made, before any images are disclosed (see "Access" at section 10 below).

CCTV monitoring of public areas, for security purposes will be conducted in a manner consistent with all existing policies adopted by the Company.
Video monitoring of public areas, for security purposes, within Company premises, is limited to uses that do not violate the reasonable expectation to privacy.

6. Lawful basis For processing

The use of CCTV is necessary in order to protect the legitimate interests of the Company. Specifically, these legitimate interests include:
protecting Company buildings and assets, both during and after hours; and
promoting the health and safety of staff and visitors; and
for disciplinary purposes.
The Data Protection Law requires that personal data are adequate, relevant and not excessive for the purpose for which they are collected. This means that the Company needs to be able to justify the obtaining and use of personal data by means of CCTV.
The use of CCTV to control the perimeter of a building for security purposes has been deemed to be justified by the Company. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.
Information may be used as part or in conjunction of an investigation process and all relevant parties will have the opportunity to view and comment on such footage. Example of the use of CCTV footage for disciplinary purposes include but are not limited to; establishing the facts of an alleged incident where other evidence is in conflict; as evidence for alleged incidents of stock loss, theft or misuse of time and attendance system; as evidence of health and safety incidents. It will not generally be used for on-going performance management purposes.

7. Location of cameras

The Company has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas shall be positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

8. Notification – signage

A copy of this Policy is available on request to employees and visitors to the Company's premises. This Policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for use of CCTV.
Signage is in place at each location in which CCTV cameras are sited to indicate that CCTV is in operation. Signage shall include the name and contact details of the data controller.

WARNING
CCTV cameras in operation

The data controller is [Company]
For more information contact [phone number]

9. Storage & retention

The Data Protection Law provide that personal data shall not be kept for longer than is necessary for the purposes for which they were obtained. The images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.
The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel.
In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out in this Policy. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.
Recorded CCTV images will be stored in a secure environment with a log of access to tapes kept. Access should be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

10. Access

Recorded footage and the monitoring equipment must be securely stored in a restricted area. Unauthorised access to that area must not be permitted at any time. The area should be locked when not occupied by authorised personnel. A log of access to images must be maintained.
In relevant circumstances, CCTV footage may be disclosed:
to An Garda Síochána where the Company (or its agents) are required by law to make a report regarding the commission of a suspected crime;
following a request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Company property;
to data subjects (or their legal representatives), pursuant to an access request under the Data Protection Acts where the time, date and location of the recordings is furnished to the Company;
to individuals (or their legal representatives) subject to a court order or another legal obligation;
to the Company's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property; and/or
to certain other bodies/agencies where the Company is required to do so or where it is necessary for the Company to do so.
On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted, and provided also that an exemption/prohibition under the Data Protection Acts does not apply to the data in question. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable.
To exercise their right of access, a data subject must make an application in writing to the Company. The Company must respond within one month.
A person should provide all the necessary information to assist the Company in locating the recorded CCTV images, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be "personal data" and may not be disclosed by the Company.

In giving a person a copy of their data, the Company may provide a still/series of still pictures or a disk, USB or other data storage device containing relevant images. However, other people's images will be obscured before the data are released.

11. Responsibilities

The Company will:
ensure that the use of CCTV is implemented in accordance with this Policy;
oversee and co-ordinate the use of CCTV within the premises for the purposes set out in this Policy;
review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this Policy;
maintain a record of access (e.g. an access log) to or the release of any material recorded or stored in the system;
ensure that the perimeter of view from fixed location cameras conforms to this Policy both internally and externally;
maintain a list of the CCTV cameras and the associated monitoring equipment and the capabilities of such equipment, located on Company premises;
ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing;
ensure that recorded CCTV images are stored in a secure place with access by authorised personnel only; and
ensure that recorded CCTV images are stored for a period not longer than 30 days and will then be erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by [title] of the Company.

12. Security companies

Where the CCTV system is controlled by a security company contracted by the Company, the Company will have a written contract with the security company in place which details the areas to be monitored, how long data is to be stored, what the security company may do with the data and what security standards are to be in place regarding the system and the recorded CCTV images.

13. Implementation & review

The date from which the Policy will apply is 25th May 2018. The Bord na Móna Policy Working Group will monitor the implementation of the Policy. The Policy will be reviewed and evaluated from time to time. Ongoing review and evaluation will take cognisance of changing law or guidelines (e.g. from the Office of the Data Protection Commissioner, An Garda Síochána, etc.), as well as feedback from staff and others.
If you have any comments or queries on this policy or the Company's implementation of CCTV, please contact informationofficer@bnm.ie.

SCHEDULE 6

Data Subject Rights

Description	When is this right applicable?
Right of access to Personal Data You have the right to receive a copy of the Personal Data we hold about you and information about how we use it.	This right is applicable at all times when we hold your Personal Data (subject to certain exemptions).
Right to rectification of Personal Data You have the right to ask us to correct Personal Data we hold about you where it is incorrect or incomplete.	This right is applicable at all times when we hold your Personal Data (subject to certain exemptions).
Right to erasure of Personal Data This right entitles you to request that your Personal Data be deleted or removed from our systems and records. However, this right only applies in certain circumstances.	Examples of when this right applies to Personal Data we hold include (subject to certain exemptions): when we no longer need the Personal Data for the purpose we collected it; if you withdraw consent to our use of your information and no other legal justification supports our continued use of your information; if you object to the way we use your information and we have no overriding grounds to continue using it; if we have used your Personal Data unlawfully; and if the Personal Data needs to be erased for compliance with law.
Right to restrict processing of Personal Data You have the right to request that we suspend our use of your Personal Data. Where we suspend our use of your Personal Data we will still be permitted to store your Personal Data, but any other use of this information will require your consent, subject to certain exemptions.	You can exercise this right if: you think that the Personal Data we hold about you is not accurate, but this only applies for a period of time that allows us to consider if your Personal Data is in fact inaccurate; the Processing is unlawful and you oppose the erasure of your Personal Data and request the restriction of its use instead;

	we no longer need the Personal Data for the purposes we have used it to date, but the Personal Data is required by you in connection with legal claims; or you have objected to our processing of the Personal Data and we are considering whether our reasons for processing override your objection.
Right to data portability This right allows you to obtain your Personal Data in a format which enables you to transfer that Personal Data to another organisation. You may have the right to have your Personal Data transferred by us directly to the other organisation, if this is technically feasible.	This right will only apply: to Personal Data you provided to us; where we have justified our use of your Personal Data based on: o your consent; or o the fulfilment by us of a contract with you; and if our use of your Personal Data is by electronic means.
Right to object to processing of Personal Data You have the right to object to our use of your Personal Data in certain circumstances. However, we may continue to use your Personal Data, despite your objection, where there are compelling legitimate grounds to do so or we need to use your Personal Data in connection with any legal claims.	
Rights relating to automated decision making and Profiling You have the right not to be subject to a decision which is based solely on automated processing (without human involvement) where that decision produces a legal effect or otherwise significantly affects you. This right means you can request that we involve one of our employees or representatives in the decision making process.	This right is not applicable if: we need to make the automated decision in order to enter into or fulfil a contract with you; we are authorised by law to take the automated decision; or the decision is based on your explicit consent.
Right to withdraw consent to processing of Personal Data Where we have relied upon your consent to process your Personal Data, you have the right to withdraw that consent.	This right only applies where we process Personal Data based upon your consent.

Right to complain to the relevant data protection authority If you think that we have processed your Personal Data in a manner that is not in accordance with data protection law, you can make a complaint to the data protection regulator. If you live or work in an EEA member state, you may complain to the regulator in that state.	This right applies at any time.