eni international resources

GDPR
Protecting your data

Notice

Recruitment Privacy Notice

Privacy and Data Protection | May 2018

Introduction

This Recruitment Privacy Notice applies to individuals who are seeking employment with Eni International Resources Limited ("EIRL"). This may include recruitment carried out for other Eni entities.

For the avoidance of doubt, this Recruitment Privacy Notice does not apply to EIRL's Staff when they apply for internal roles.

If you accept an offer of employment with EIRL, you also should refer to the EIRL Staff Privacy Notice for information about how we process Staff personal data.

This Recruitment Privacy Notice describes how we collect, use and process your personal data, and how, in doing so, we comply with our legal obligations to you.

For the purpose of applicable data protection legislation (including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), EIRL is the company responsible for your personal data ("EIRL" or "us"). Please refer to Annex 1.

This Recruitment Privacy Notice is not contractual and may be amended or removed from time to time. Any changes in our approach to data privacy will be posted accordingly.

If you are dissatisfied with any aspect of our Recruitment Privacy Notice, you may have legal rights and so, where relevant, we have described these as well.

Definitions

Delete – In this day and age, it is virtually impossible to guarantee the permanent and irretrievable deletion of electronic data. In addition, as we have explained to you in this Recruitment Privacy Notice, sometimes we may be obliged by law or regulation, or need for risk-management reasons, to retain the ability to access certain elements of personal data. However, our commitment to you is that once your personal data reaches the end of its nominal retention period, or where we receive a valid request from you to erase it, we will put in place specific operational and Systems measures to ensure that your data is "put beyond use". By this we mean that while the data will still technically exist on an archive system, we will ensure that it cannot be accessed by any of our operational Systems, processes or Staff. Only a very (and we mean exceptionally) small number of senior Staff, in very (and, again, we mean exceptionally) limited and carefully prescribed situations, be able to restore your personal data so that it can be viewed for those legitimate purposes. Once we are clear that all relevant legally mandated retention periods have expired (which, for present purposes, we expect to be the period of up to nine months, unless we are legally required to hold your personal data for longer than this), we will take the additional final step of undertaking a "hard delete", whereby not even that very limited number of senior Staff would be able to restore your personal data.

General Data Protection Regulation (the "GDPR") – a European Union statutory instrument which aims to harmonise European data protection laws. It has an effective date of 25 May 2018, and any references to it should be construed to include any national legislation implementing it.

Recruitment – this refers to individuals who are seeking employment as members of EIRL's Staff.

Sensitive Personal Data – this is personal data consisting of information such as your racial or ethnic origin, your political opinions or religious beliefs, whether you are a trade union member, your physical and mental health, your genetic and biometric data, data relating to your sex life and sexual orientation, and whether you have or are alleged to have committed a criminal offence. Due to the nature of sensitive personal data, data protection legislation is much stricter about how such data should be held and processed. We will only process your sensitive personal data where appropriate and in accordance with local law requirements.

Staff – includes former and current employees engaged (or who have accepted an offer to be engaged) directly in the business of EIRL (including any expats) as well as certain other workers engaged or previously engaged in the business of providing services to EIRL (even though they are not classed as employees).

Systems – include telephone, computer, internet and Wi-Fi systems, software and portals, accounts and/or networks belonging, controlled or used by EIRL that are used to transmit, undertake and/or receive communications or are otherwise used in the course of EIRL's business, including EIRL's candidate portal software.

What kind of Personal Data do we collect about recruitment?

We collect data about you to enable the Recruitment process to run smoothly, for example where we have a legitimate interest when considering you for a role and to ensure that we are able to comply with our legal and regulatory obligations. Depending on the relevant circumstances and applicable local laws and requirements, we may collect some or all of the information listed below to help us with this, where appropriate:

- name
- age/date of birth
- contact details, such as address, email address and telephone number
- birth identification number
- sex/gender
- photograph
- marital status and information regarding any dependants
- CV

- education details and training certificates
- employment history, locations of previous employment, geographical preferences and availability for future employment and professional areas of interest
- source of application
- referee details
- your signature, including in electronic form
- immigration status (whether you need a work permit)
- nationality/citizenship/place of birth
- a copy of your driving licence and/or passport/identity card
- social security number (or equivalent in your country) and any other tax-related information
- details about your current or former role(s) including remuneration, pension and benefits arrangements, contractual notice period and expected remuneration
- extra information that you choose to tell us
- extra information that your referees choose to tell us about you
- any additional information required by local legislation, and
- information regarding any pending convictions or criminal proceedings, administrative penalties or civil judgements of conviction issued against you
- family or kinship relationship with any Public Officials or top management members of companies, consortia, foundations or associations that carry out professional and business activities of particular interest to Eni
- extra information that we find from other third party sources.

Please note that the above list of the categories of personal data which we collect is not exhaustive.

We will process some or all of the above items of personal data to ensure the Recruitment process can run smoothly and so that we can make an informed decision about your suitability for the role in question (or other appropriate roles that may be available, depending on the circumstances).

Depending on the type of personal data in question and the grounds on which we may be processing it, should you decline to provide us with such data, we may not be able to continue with the Recruitment process.

For details of the legal bases that we rely on to be able to use and process your personal data, please see the section below entitled "Legal bases for us processing your data".

How do we collect your Personal Data?

We collect your personal data in three primary ways:

1. Personal data that you give to us;
2. Personal data that we receive from other sources; and
3. Personal data we collect automatically.

Below are some more details about each of these methods.

Personal data you give to us

EIRL needs to know certain information about you in order to properly conduct the Recruitment process.

There are numerous ways that you can share your information with us. Where appropriate and in accordance with any local laws and requirements, these may include:

- When you make a job application to EIRL via this portal;
- When you make a job application to EIRL via job boards;
- When you make a job application to EIRL via networking websites (such as LinkedIn);
- Information you provide to EIRL's Staff in communications during the Recruitment process.

Personal data we receive from other sources

We also receive personal data about you from other sources. Depending on the relevant circumstances and applicable local laws and requirements, these may include personal data received in the following situations:

- information obtained about you when we searched third party sources such as LinkedIn and other job sites for potential Recruitment for roles at EIRL
- when a member of EIRL's Staff refers you to us via our Recruitment team, they will share personal information about you with us

- if you were referred to us through a recruitment agency or consultant, they may have shared personal information about you with us
- information obtained about you from third party service providers who undertake background checks about you on our behalf
- your referees may disclose personal information about you to us, and
- if you 'like' our page on Facebook or 'follow' us on Twitter or interact with us on any other social media platform, we will receive your personal information from those sites.

Personal data we collect automatically

Where appropriate and in accordance with any local laws and requirements, we may collect your personal data automatically the following ways:

- communications that you send to EIRL which pass through EIRL's Systems, including emails, instant messages, social media posts, text messages and app-based messages (such as WhatsApp)
- when you visit our website, your IP address, the date and the times and frequency with which you access the website and the way you browse its content. We will also collect data from you when you contact us via the website, for example by using the chat function.

How do we use your Personal Data?

We generally use Recruitment data in the following ways:

1. To ensure the smooth running of the Recruitment process
2. Assessing your suitability for job roles
3. To undertake equal opportunities monitoring
4. To help us to establish, exercise or defend legal claims; and
5. To help us to help you and to understand our legal obligations if you suffer from a health condition or disability.

Below are some more details about each of these purposes.

To ensure the smooth running of the Recruitment process:

We have listed below various ways in which we may process or use your personal data for this purpose, where appropriate and in accordance with any local laws and requirements:

- Collecting your data from you and other sources, such as your referees;
- Passing on your details to recruiters who assist us with finding new members of Staff;
- Enabling recruiters to contact you about the role;
- Enabling our hiring managers to decide whether to make you a job offer;
- Determining the terms on which you will work for us;
- Assessing your qualifications for a particular job or task, including decisions about appointment;
- Informing you of the result of your job application;
- Verifying information we have received, using third party resources (such as psychometric evaluations or skills tests) or through information requests (such as references, qualifications and potentially any criminal convictions, to the extent that this is appropriate and in accordance with local laws);
- To satisfy EIRL's pre-employment checks, including checking references, criminal records, and drug testing and any other background checks required by EIRL;
- To prevent detrimental situations from occurring that may expose Eni to the risk of corruption offences being committed and to avoid potential conflicts of interest;
- Storing and transferring your details (and updating them when necessary);
- Complying with our legal obligations in connection with the detection of crime or the collection of taxes or duties;
- Keeping a record of when you attend an interview or other assessment;
- When making arrangements in order to offer you a job;
- Carrying out satisfaction surveys on our Recruitment process;
- Monitoring communications that you send to EIRL which pass through EIRL's Systems, including emails, instant messages, social media posts, text messages and app-based messages (such as WhatsApp);

- Keeping a record of security data so that we can be sure who is on our premises at any given time;
- Running CCTV at our premises to ensure the safety and security of our Staff and property;
- Carrying out any other obligations or necessary requirements arising from the Recruitment process; and
- If you are successful in the role, transferring your personal data onto our internal HR system.

Assessing your suitability for job roles

In addition to the usual human resources processes, as technology advances, it may be possible in the future for us to use machine learning, profiling and algorithms to help us to make Recruitment decisions and to more accurately assess your suitability for job roles and to help us make other decisions in our Recruitment processes. In relevant circumstances, and where legally permissible, we may require your consent to carry out some of these activities and will provide further details in relation to this.

To undertake equal opportunities monitoring

We are committed to ensuring that our Recruitment processes are aligned with our approach to equal opportunities. Some of the data we may collect about you (in appropriate circumstances and where permissible in accordance with local law and requirements) comes under the umbrella of "diversity information". This could be information about your ethnic background, gender, disability, age, sexual orientation, religion or other beliefs, child care / carer arrangements and/or social-economic background. Where appropriate and in accordance with local law and requirements, we'll use this information on an anonymised basis to monitor our compliance with equal opportunities.

To help us to establish, exercise or defend legal claims

In more unusual circumstances, we may use your personal data to help us to establish, exercise or defend legal claims.

To help us to help you and to understand our legal obligations if you suffer from a health condition or disability

If you suffer from any health conditions or disabilities, we may, subject to local laws and requirements, record details of them so that we can make reasonable adjustments to interview and other Recruitment procedures if required.

Please note that the above list of the ways in which we use your personal data for this purpose is not exhaustive.

We will only use your personal data for the purposes for which we collect 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 data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

To find out more about the legal bases that we rely on to be able to use and process your personal data in the above ways, please see the section below entitled "Legal bases for us processing your data".

Who do we share your Personal Data with?

Where appropriate and in accordance with local laws and requirements, we may share certain personal data, in various ways and for various reasons, with the following categories of people:

- any of our group companies and joint venture partners (this may include those in our overseas sites);
- external third party organisations (for example those which carry out psychometric testing), business associates and professional advisers, to enable us to assess your suitability for the role;
- where relevant, recruiters who will help us to find the right role for you;
- individuals and organisations who hold information related to your reference or application to work with us, such as current, or past employers, educators and examining bodies, immigration agencies and employment and recruitment agencies;
- third parties, in order to comply with our legal obligations;
- third parties who hold information related to your financial record such as financial organisations, credit reference agencies and debt collection and tracing agencies;
- where appropriate, medical professionals such as your GP or an occupational health specialist;
- third party service providers who perform functions on our behalf (including external consultants, business associates and professional advisers such as lawyers, auditors, accountants, technical support functions and IT consultants carrying out testing and development work on our business technology systems;
- third party outsourced IT and document storage providers where we have an appropriate processing agreement (or similar protections) in place;
- third parties involved in, or assisting with, litigation (including legal advisers, witnesses, experts and judicial and quasi-judicial authorities);

- third parties who we have retained to provide services such as reference, qualification and criminal convictions checks, to the extent that these checks are appropriate and in accordance with local laws; and
- if EIRL merges with or is acquired by another business or company in the future, (or is in meaningful discussions about such a possibility) we may share your personal data with the (prospective) new owners of the business or company.

How do we safeguard your Personal Data?

We care about protecting your information. That's why we put in place appropriate measures that are designed to prevent unauthorised access to, and misuse of, your personal data. These include measures to deal with any suspected data breach.

We are committed to taking all reasonable and appropriate steps to protect the personal data that we hold from misuse, loss, or unauthorised access. We do this by having in place a range of appropriate technical and organisational measures.

If you suspect any misuse or loss of or unauthorised access to your personal data please let us know immediately. Details of how to contact us can be found in Annex 1.

How long do we keep your Personal Data for?

Subject to your rights (as explained in this Notice) we will ordinarily process your data from when you first contact us and retain it for a period until after the Recruitment process ends. The precise length of time will depend the type of data, our legitimate business needs and other legal or regulatory rules that may require us to retain it for certain minimum periods.

We would normally hold your data for around 2 years after determination that you have been unsuccessful for the role, but we will retain your data for up to 5 years for the purposes of considering you for other roles if you were involved in a selection process or unless you indicate to us during the recruitment process that you do not wish us to do so.

We may be required to retain your data for a longer period to comply with obligations imposed by immigration authorities.

In determining the appropriate retention period for different types of personal data, we always consider the amount, nature, and sensitivity of the personal data in question, the potential risk of harm from unauthorised use or disclosure of that personal data, the purposes for which we need to process it and whether we can achieve those purposes by other means (in addition of course to ensuring that we comply with our legal, regulatory and risk-management obligations, as described above).

Once we have determined that we no longer need to hold your personal data, we will Delete it from our Systems.

How can you access, amend or take back the Personal Data you that you have given to us?

One of the GDPR's main objectives is to protect and clarify the rights of EU citizens and individuals in the EU with regard to data privacy. Even if we already hold your personal data, you still have various rights in relation to it, which we have set out below.

To get in touch about these rights (including if you wish to exercise any of them), please contact us using the details listed in Annex 1. We will seek to deal with your request without undue delay, and in any event within one month (subject to any extensions to which we are lawfully entitled). Please note that we may keep a record of your communications to help us resolve any issues which you raise.

The GDPR gives you the following rights in relation to your personal data:

Right to object

This right enables you to object to us processing your personal data where we do so for one of the following four reasons: (i) because it is within our legitimate interests (ii) to enable us to perform a task in the public interest or exercise official authority; (iii) to send you direct marketing materials; and (iv) for scientific, historical, research, or statistical purposes.

The "legitimate interests" category above is the one most likely to apply in relation to our Recruitment processes, and if your objection relates to us processing your personal data because we deem it necessary for our legitimate interests, we must act on your objection by ceasing the activity in question unless:

- we can show that we have compelling legitimate grounds for processing which overrides your interests; or
- we are processing your data for the establishment, exercise or defence of a legal claim.

Right to withdraw consent

Where we have obtained your consent to process your personal data for certain activities (for example, for automatic profiling), you may withdraw this consent at any time and we will cease to carry out the particular activity that you previously consented to unless we consider that there is an alternative legal basis to justify our continued processing of your data for this purpose, in which case we will inform you of this condition.

Right to submit a Data Subject Access Request (DSAR)

You may ask us to confirm what information we hold about you at any time, and request us to modify, update or Delete such information. We may ask you for more information about your request. If we provide you with access to the information we hold about you, we will not charge you for this unless your request is "manifestly unfounded or excessive". If you request further copies of this information from us, we may charge you a reasonable administrative cost, where legally permissible. Where we are legally permitted to do so, we may refuse your request. If we refuse your request we will tell you the reasons for doing so.

Right to erasure

You have the right to request that we "erase" your personal data in certain circumstances. Normally, the information must meet one of the following criteria:

- the data are no longer necessary for the purpose for which we originally collected and/or processed them;
- where previously given, you have withdrawn your consent to us processing your data, and there is no other valid reason for us to continue processing;
- the data has been processed unlawfully (i.e. in a manner which does not comply with the GDPR);
- it is necessary for the data to be erased in order for us to comply with our obligations as a data controller under EU or Member State law; or
- if we process the data because we believe it necessary to do so for our legitimate interests, you object to the processing and we are unable to demonstrate overriding legitimate grounds for our continued processing.

We would only be entitled to refuse to comply with your request for erasure for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with legal obligations or for the performance of a public interest task or exercise of official authority;
- for public health reasons in the public interest;
- for archival, research or statistical purposes; or
- to exercise or defend a legal claim.

When complying with a valid request for the erasure of data, we will take all reasonably practicable steps to Delete the relevant data.

For the avoidance of doubt, deleting your online profile will not erase all of your personal data held by us. If you wish to request that we erase your personal data, details of how to contact us can be found in Annex 1.

Right to restrict processing

You have the right to request that we restrict our processing of your personal data in certain circumstances. This means that we can only continue to store your data and will not be able to carry out any further processing activities with it until either: (i) one of the circumstances listed below is resolved; (ii) you consent; or (iii) further processing is necessary for either the establishment, exercise or defence of legal claims, the protection of the rights of another individual, or reasons of important EU or Member State public interest.

The circumstances in which you are entitled to request that we restrict the processing of your personal data are:

- where you dispute the accuracy of the personal data that we are processing about you. In this case, our processing of your personal data will be restricted for the period during which the accuracy of the data is verified;
- where you object to our processing of your personal data for our legitimate interests. Here, you can request that the data be restricted while we verify our grounds for processing your personal data;
- where our processing of your data is unlawful, but you would prefer us to restrict our processing of it rather than erasing it; and
- where we have no further need to process your personal data but you require the data to establish, exercise, or defend legal claims.

If we have shared your personal data with third parties, we will notify them about the restricted processing unless this is impossible or involves disproportionate effort. We will, of course, notify you before lifting any restriction on processing your personal data.

Right to rectification

You also have the right to request that we rectify any inaccurate or incomplete personal data that we hold about you, including by means of providing a supplementary statement. If we have shared this personal data with third parties, we will notify them about the rectification unless this is impossible or involves disproportionate effort. You may also request details of the third parties that we have disclosed the inaccurate or incomplete personal data to. Where we think that it is reasonable for us not to comply with your request, we will explain our reasons for this decision.

Right of data portability

If you wish, you have the right to transfer your personal data between data controllers. In effect, this means that you are able to transfer the details we hold on you to another potential employer or a third party. To allow you to do so, we will provide you with your data in a commonly used machine-readable format so that you can transfer the data to another potential employer. Alternatively, we may directly transfer the data for you. This right of data portability applies to: (i) personal data that we process automatically (i.e. without any human intervention); (ii) personal data provided by you; and (iii) personal data that we process based on your consent or in order to fulfil a contract.

Right to lodge a complaint with a supervisory authority

You also have the right to lodge a complaint with your local supervisory authority. Details of how to contact them can be found in Annex 2.

If you would like to exercise any of these rights, or withdraw your consent to the processing of your personal data (where consent is our legal basis for processing your personal data), details of how to contact us can be found in Annex 1. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

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 the period for which we hold your data.

Who is responsible for processing your Personal Data?

EIRL is responsible for processing your personal data and you can find the details where it is located and how to get in touch in Annex 1.

If you have any comments or suggestions concerning this Recruitment Privacy Notice please contact us using the details in Annex 1. We take privacy seriously so we'll get back to you as soon as possible.

How do we store and transfer your data internationally?

EIRL is a global organisation. In order for us to continue operating in this way and to carry out the purposes described in this Recruitment Privacy Notice, your data may be transferred to the following recipients located outside of your jurisdiction:

- between and within Eni entities and joint ventures;
- to a cloud-based storage provider; and
- to other third parties, as referred to above under "Who do we share your personal data with?"

We want to make sure that your data is stored and transferred in a way which is secure. We will therefore only transfer data outside of the European Economic Area or EEA (i.e. the Member States of the European Union, together with Norway, Iceland and Liechtenstein) where it is compliant with data protection legislation and the means of transfer provides adequate safeguards in relation to your data, for example:

- by way of data transfer agreement, incorporating the current standard contractual clauses adopted by the European Commission for the transfer of personal data by data controllers in the EEA to data controllers and processors in jurisdictions without adequate data protection laws;
- by signing up to the EU-U.S. Privacy Shield Framework for the transfer of personal data from entities in the EU to entities in the United States of America or any equivalent agreement in respect of other jurisdictions;
- where we are transferring your data to a country where there has been a finding of adequacy by the European Commission in respect of that country's levels of data protection via its legislation;
- where it is necessary for the conclusion or performance of a contract between ourselves and a third party and the transfer is in your interests for the purposes of that contract (for example, if we need to transfer your data to a benefits provider based outside the EEA); or
- where you have consented to the data transfer.

To ensure that your personal information receives an adequate level of protection, we have put in place appropriate procedures with the third parties we share your personal data with to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the law on data protection.

Legal bases for us processing your data

There are a number of different ways that we are lawfully able to process your personal data. We have set these out below.

Where processing your personal data is within our legitimate interests

Article 6(1)(f) of the GDPR says that we can process your data where it "is necessary for the purposes of the legitimate interests pursued by [us] or by a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of [you] which require protection of personal data."

We consider the following to be non-exhaustive examples of processing activities that are in our legitimate interests to carry out so that we can run a successful Recruitment process:

- assessing your suitability for a role at EIRL;
- informing you of the result of your job application;
- for our internal administrative purposes;
- to pass to medical professionals overseas;
- to make appropriate background checks; and
- to assist us with establishing, exercising or defending legal claims.

You can find further examples of ways in which we process your personal data for the purposes of our legitimate interests in the non-exhaustive list above under the heading, "To ensure the smooth running of our recruitment process".

Where processing your personal data is necessary for us to carry out our legal obligations

As well as our obligations to you that arise in connection with our Recruitment processes, we also have other legal obligations that we need to comply with. Article (6)(1)(c) of the GDPR states that we can process your personal data where this processing "is necessary for compliance with a legal obligation to which [we] are subject".

Examples of our legal obligations can be found in the non-exhaustive list set out above under the heading, "To ensure the smooth running of our recruitment processes".

Where processing your Sensitive Personal Data is necessary for us to exercise our rights or carry out our employment and social security law obligations

Sometimes it will be necessary for us to process your Sensitive Personal Data during the course of the Recruitment process. Article 9(2)(b) of the GDPR allows us to do this where the processing is "necessary for the purposes of carrying out the obligations and exercising [our or your] specific rights... in the field of employment and social security and social protection law", as long as this is allowed by law.

We process your Sensitive Personal Data for the purpose of ensuring our compliance with our equal opportunities obligations where this in accordance with local law, but we may also process other elements of your Sensitive Personal Data during the course of the Recruitment process for other reasons. You can find out how we process your Sensitive Personal Data in the context of the Recruitment process in the non-exhaustive list under "To ensure the smooth running of the Recruitment process".

Where appropriate and in accordance with any local laws and requirements, we may also process your medical data to enable us to provide you with adequate support if you suffer from a health condition or disability, in order to determine any reasonable adjustments to interview or other Recruitment procedures. You can find out more about this under the section "To help us to establish, exercise or defend legal claims."

Where processing your personal data is necessary for us to establish, exercise or defend legal claims

Sometimes it may be necessary for us to process personal data and Sensitive Personal Data in connection with exercising or defending legal claims. Article 9(2)(f) of the GDPR allows this where the processing "is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity".

This may arise for example where we need to take legal advice in relation to legal proceedings or are required by law to preserve or disclose certain information as part of the legal process.

Where you give us your consent to process your Personal Data

In very limited circumstances, we are required to obtain your opt-in consent before we can undertake certain processing activities with your personal data. Article 4(11) of the GDPR states that opt-in consent is "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." In plain language, this means that:

- you have to give us your consent freely, without us putting you under any type of pressure;
- you have to know what you are consenting to – so we'll make sure we give you enough information;
- you should only be asked to consent to one processing activity at a time – we therefore avoid "bundling" consents together so that you don't know exactly what you're agreeing to; and
- you need to take positive and affirmative action in giving us your consent – we're likely to provide a tick box for you to check so that this requirement is met in a clear and unambiguous fashion.

As and when we introduce these processing activities requiring your consent, we will provide you with more information so that you can decide whether you want to opt-in.

You have the right to withdraw your consent to these activities. You can do so at any time, and details of how to do so can be found above in the section entitled, "Right to withdraw consent".

We don't think that any of the above activities prejudice you in any way. However, you do have the right to object to us processing your personal data in certain circumstances. If you would like to know more about these circumstances and how to object to our processing activities, please see the subsection entitled "Right to object".

Annex 1

How you can get in touch with us:

- to access, amend or take back the personal data that you have given to us;
- if you suspect any misuse or loss of or unauthorised access to your personal information;
- to withdraw your consent to the processing of your personal data (where consent is the legal basis on which we process your personal data);
- with any comments or suggestions concerning this Recruitment Privacy Notice.

You can write to us at the following address:

Data Protection Team,
Eni International Resources Ltd
10 Ebury Bridge Road
London SW1W 8PZ

Alternatively, you can send an email to: eirl.dataprotection@eni.com

Annex 2 - How to contact your Local Supervisory Authority

Country in which you apply to become a member of EIRL's Staff:	UK
Details of your local supervisory authority:	The Information Commissioner's Office. You can contact them in the following ways: **Phone:** 0303 123 1113 **Email:** casework@ico.org.uk **Live chat:** https://ico.org.uk/global/contact-us/live-chat **Post:** Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF