Petredec

Data Protection Policy

Issued By	Director of Corporate Operations
Issued Date	March 2026
Version	1

We are LPG

DATA PROTECTION POLICY

This Data Protection Policy applies to Petredec Group Limited and subsidiaries (together "Petredec"), in all jurisdictions in which we operate, except in any jurisdiction which is subject to its own policy.

INTERPRETATION – DEFINITIONS:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Protection Principles: principles by which Petredec processes Personal Data, so far as may be relevant in a given jurisdiction, these being:

- It is processed lawfully, fairly and in a transparent manner.
- It is collected only for specified, explicit and legitimate purposes.
- It is only processed where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- It is accurate and, where necessary, kept up-to-date and Petredec takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- It is kept only for the period necessary for processing.
- Appropriate measures are adopted to make sure that it is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be (i) nationals or (ii) residents of any country and may have legal rights regarding their Personal Data or (iii) juristic persons, limited to certain territories.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): the individual appointed from time to time (contactable at: dpo@petredec.com) who is responsible for administering this Data Protection Policy for Petredec Group, except where a separate DPO has been appointed for a specific jurisdiction. For the name of the current DPO, and a full list of any jurisdiction-specific DPOs (with their names and contact details), please refer to DPO Contact Information link https://petredec.com/dpo-contact-information.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Information Systems: information assets (e.g. databases, files), software assets (e.g. applications and systems software and development tools), and hardware assets (e.g. computers, communications equipment and magnetic media), taken together.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of:

a) general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or
b) stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates

cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

PETREDEC'S PRIVACY POLICY AND STATEMENT

Petredec is committed to protecting your privacy. You can visit most pages on our website without giving us any information about yourself. But sometimes we do need information to provide services that you request, and this Privacy Statement explains data collection and use in those situations.

This Privacy Statement only applies to Petredec; it does not apply to other online or offline websites, products or services. Please read the complete Privacy Policy and Statement.

Petredec is committed always to acting in accordance with Data Protection Principles wherever these may be relevant. Where it departs from Data Protection Principles, it shall do so only insofar as such activity is lawful in the given jurisdiction, and all commitments made in this Data Protection Policy shall be subject to this.

COLLECTION OF YOUR PERSONAL DATA

We will ask you when we need information that personally identifies you (Personal Data) or allows us to contact you. Generally, this information is requested when you are registering before entering a contest, ordering e-mail newsletters, signing up for an event or training, or when purchasing and/or registering for any of our products. Personal Data collected by Petredec often is limited to e-mail address, language, country or location, but may include other information when needed to provide a service you requested.

Petredec also collects certain Information from your computer hardware and software. This information may include: your IP address, browser type, operating system, domain name, access times and referring website addresses. This information is used for the operation of the service, to maintain quality of the service, and to provide general statistics regarding use of Petredec's website.

Petredec also collects information about which pages our customers visit within our Web. This website visitation data is identified only by a unique I.D. number, and it is never linked with Personal Data unless a user consents as described below.

USE OF YOUR PERSONAL DATA

We use your Personal Data for the following purposes:

1. To ensure our website is relevant to your needs.
2. To help us create and publish content most relevant to you.

We will merge site-visitation data with anonymous demographic information for research purposes, and we may use this information in aggregate to provide more relevant content. In some limited-entry sections, with your approval, we will combine site-visitation data with your Personal Data in order to provide you with personalised content. If you decline permission, we will not provide you the personalised service and won't merge your Personal Data with site-visitation data.

We occasionally appoint other businesses to provide limited services on our behalf, including packaging, mailing and delivering purchases, answering customer questions about products or services, sending postal mail and processing event registration. We will only provide those businesses the information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Petredec may disclose your Personal Data if required to do so by law or in the good-faith belief that such action is necessary to:

1. conform to the edicts of the law or comply with legal process served on Petredec or the website;
2. protect and defend the rights or property of Petredec and its website; or
3. act in urgent circumstances to protect the personal safety of Petredec's employees, users of our products or services or members of the public.

CONTROL OF YOUR PERSONAL DATA

When you register, or otherwise give us Personal Data, Petredec will not share that information with Third Parties without your permission, other than for the limited exceptions already listed. It will only be used for the purposes stated above.

ACCESS TO YOUR PERSONAL DATA

We will provide you with the means to ensure that your Personal Data is correct and current.

Some services offered on Petredec's website may collect information that is not accessible via the Home or Profile page. However, in such cases, you can access your Personal Data by contacting Petredec.

SECURITY OF YOUR PERSONAL DATA

Petredec is committed to protecting the security of your Personal Data. We use a variety of security technologies and procedures to help protect your Personal Data from unauthorised access, use or disclosure. For example, we store the Personal Data you provide in computer servers with limited access that are located in controlled facilities.

USE OF COOKIES

When someone visits our website, a cookie is placed on the customer's machine (if the customer accepts cookies) or is read if the customer has visited the site previously. One use of cookies is to assist in the collection of the site visitation statistics described above.

We also use cookies to collect information on which newsletter links are clicked by customers. This information is used to ensure we are sending information customers want to read. It is collected in aggregate form and never linked with your Personal Data.

Web beacons, also known as clear gif technology, or action tags, may be used to assist in delivering the cookie on our site. This technology tells us how many visitors clicked on key elements (such as links or graphics) on Petredec's website. We do not use this technology to access your personally identifiable information on our website; it is a tool we use to compile aggregated statistics about Petredec's website usage. We may share aggregated site statistics with partner businesses but do not allow other businesses to place clear gifs on our website.

If you choose to not have your browser accept cookies from Petredec's website, you will be able to view the text on the screens, however you will not experience a personalised visit nor will you be able to subscribe to the service offerings on the site.

OPT-OUT PROCEDURE

"Opting-out" in a legal sense means the same as it does in an everyday sense. To "Opt-Out" means you are choosing to no longer participate in something.

Opting out becomes significant in a legal sense when you develop a website or app that's legally required to provide a method of opting out to those who use your website or app. Not all business models are required by law to provide an opt-out method for customers.

An opt-out procedure lets customers know that they have the ability and right to opt out of aspects of a website or app, as well as a clear and easy-to-follow method for actually opting out, and is required by law in certain circumstances.

PURPOSE SPECIFICATION OF PERSONAL DATA

Any Personal Data supplied by a Data Subject shall only be collected and used by Petredec for the purpose for which it was originally intended. In the event that the Personal Data will be used for another purpose, consent from the Data Subject will be obtained prior to the use of such information.

ACCURACY OF PERSONAL DATA

In the event of any changes to the Personal Data of a Data Subject, the Data Subject is under an obligation to inform Petredec of the said changes within a reasonable period of time.

DOCUMENT RETENTION AND RECORD OF PROCESSING

It is Petredec's policy to maintain – so far as may be relevant – complete, accurate and quality records including records consisting of Personal Data of Data Subjects. In accordance with Data Protection Principles, records are to be retained for the period of their immediate use, unless longer retention is required for historical reference, contractual, legal or regulatory requirements or for other purposes as may be set forth below. Records that are no longer required, or have satisfied their required periods of retention, shall be destroyed.

Company Personnel shall not knowingly destroy a document with the intent to obstruct or influence the investigation or proper administration of any matter within the jurisdiction of any government department or agency or in relation to or contemplation of any such matter or case.

LEGAL HOLD ON DOCUMENTS

From time to time, the Data Protection Officer may issue a "legal hold", suspending the destruction of any records due to pending, threatened, or otherwise reasonably foreseeable litigation, audits, government investigations, or similar proceedings. If and when Company Personnel are informed of this by the Data Protection Officer, they should not discard any documents relevant to the subject matter of the lawsuit, investigation or proceeding.

Relevant Company Personnel will be informed of the specific types of documents that are relevant and must be retained for these purposes by the Data Protection Officer. Until that point in time, document that may be relevant should not be discarded without the written approval of the Data Protection Officer. If in doubt, save the document.

In all circumstances, documents and personal data must be retained only for as long as necessary to fulfil the purposes for which they were collected, including to meet applicable legal, regulatory, tax, accounting, and operational requirements in the relevant jurisdiction(s).
Retention periods may vary depending on the nature of the data, the business activity, and the country in which Petredec operates.
Petredec maintains internal guidelines to support appropriate retention practices. These guidelines are indicative and may not cover all categories of records that may be required to be retained now or in the future.
Where there is uncertainty regarding the appropriate retention period, or where records may be relevant to an investigation, dispute, or regulatory inquiry, employees must seek guidance from the Data Protection Officer and ensure that no documents are deleted or altered until confirmation is received.
Please note that failure to follow this policy can result in possible civil and criminal sanctions against Petredec and its Officers, Directors and Employees, and possible disciplinary action against responsible individuals, up to and including termination of employment.

RECORD AND DOCUMENT DESTRUCTION

So far as may be relevant, Petredec follows specific procedures regarding the destruction and disposal of paper and electronic records and documents.

Any documents containing Personal Data or other confidential information must be destroyed so that the information cannot be practically read or reconstructed.

All paper documents must be destroyed with a cross-cut shredder.

Electronic documents, Personal Data or other confidential information must be destroyed with the appropriate software for overwriting electronic data, disk degaussing technology or through other means of physical destruction where the information cannot be practically read or reconstructed.

SUSPENSION OF RECORD AND DOCUMENT DESTRUCTION SCHEDULE

In the event Petredec is served with a subpoena or request for documents or any Company Personnel becomes aware of an investigation or audit concerning Petredec or the commencement of any litigation against or concerning Petredec, such Company Personnel shall inform Petredec and any further disposal of documents shall be suspended until such time as Petredec determines otherwise.

Petredec shall take such steps as is necessary to promptly inform appropriate Company Personnel of any suspension in the further disposal of documents.

Once the litigation is terminated or settled, Petredec will notify the appropriate individual(s) so that backup tapes can be put back into general rotation, archiving can be turned back on and copies of e-mail Data stored for the legal hold can be deleted.

DATA SECURITY

In accordance with Data Protection Principles, Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

Petredec will develop, implement and maintain safeguards appropriate to its size, scope and business, our available resources, the amount of Personal Data that it owns or maintains on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). It will carry out regular risk assessments of our activities and procedures.

Petredec will regularly evaluate and test the effectiveness of those safeguards to ensure security of its Processing of Personal Data.

Petredec will ensure that all Company Personnel maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;
(b) Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and
(c) Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

Company Personnel must not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with relevant standards to protect Personal Data.

RISK ASSESSMENT

Petredec will carry out regular risk assessments of its Information Systems using Petredec's risk management procedures. These risk assessments will examine potential vulnerabilities and security measures and will lead to the development of controls consistent with reducing the identified risk to an acceptable level.

PRIVACY BY DESIGN

Petredec shall implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

Company Personnel must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

(a) The state of the art.
(b) The cost of implementation.
(c) The nature, scope, context and purposes of Processing.
(d) The risks of varying likelihood and severity for rights and freedoms of the Data Subject posed by the Processing.

DATA PROTECTION IMPACT ASSESSMENT

Users of Petredec's Information Systems will conduct DPIAs in respect of any high-risk Processing.

Company Personnel should conduct a DPIA (and discuss any material findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(a) Use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes).

A DPIA must include:

(a) A description of the Processing, its purposes and the Controller's legitimate interests if appropriate.
(b) An assessment of the necessity and proportionality of the Processing in relation to its purpose.
(c) An assessment of the risk to individuals.
(d) The risk mitigation measures in place and demonstration of compliance.

DPIAs shall be maintained should be kept for as long as the underlying, high-risk data processing activity continues, and for a reasonable period afterward (to be approved on a case-by-case basis by the DPO).

ACCESS TO PERSONAL DATA

Petredec seeks to provide accurate and timely information regarding its activities to its clients / customers, employees, suppliers, partners and stakeholders and other interested parties, in accordance with Data Protection Principles.

In determining whether any particular Personal Data is to be made available by Petredec as a routine matter and upon request Petredec first considers whether such information falls within the scope of this Policy and if so, then determines whether there is any compelling reason not to disclose all or any part of such information, with particular regard to applicable data protection laws. In making the determination Petredec shall consider whether the disclosure of information in likely to cause harm to specific parties or interests that outweighs the benefit of disclosure, whether there is a legal requirement to disclose, or whether the information contains and makes reference to Personal Data exemptions, below which are not exhaustive.

Company Personnel must establish and maintain appropriate safeguards to respect the personal privacy of Data Subjects and protect the confidentiality of Personal Data about them.

Petredec does not provide access to the following information, except to the extent expressly permitted by Petredec's Personnel Policies, Procedures and Rules:

1. Personal Data, including personal employment records, medical information and personal communications (including e-mail) of the following individuals and their families: Chief Executive Officer of Petredec, Management, Officers, Employees and Consultants;
2. Information relating to employee appointment and selection process;
3. Information relating to proceedings of Petredec's internal conflict resolution mechanisms; and
4. Information relating to investigations of allegations of employee misconduct and personal conflicts of interest.

The Data Protection Officer of Petredec shall be responsible for administering this policy and all such requests should be addressed to the Data Protection Officer listed at the end of this policy.

PERSONAL DATA OF CUSTOMERS AND CLIENTS (FOR BOTH NATURAL PERSONS AND JURISTIC PERSONS)

Petredec does not provide access to the following customer / client information, except permitted by the customer / client Policies, Procedures and Rules:

1. Personal Data of customers / clients and their employees;
2. Financial and Credit information of customers / clients and their employees.

PERSONAL DATA OF SUPPLIERS AND THIRD PARTIES CLIENTS (FOR BOTH NATURAL PERSONS AND JURISTIC PERSONS)

Petredec does not provide access to the following suppliers and Third Parties' information, except permitted by the Supplier and Third Parties' Policies, Procedures and Rules:

1. Personal Data of Suppliers and Third Parties and their Employees;
2. Financial and Credit information of Suppliers and Third parties and their Employees.

DATA SUBJECT CONSENT

This communication should be done:

1. Whenever a new Relationship / Contract / Agreement is entered into with the Data Subject.
2. Annually to ensure that the Data Subject is aware of the Personal Data kept by Petredec.
3. Whenever there is a change in Petredec's business, functions, activities that impacts on the use of the Data Subject's Personal Data.

The Data Subject Notification confirms the purpose of the use of Personal Data and the specific Personal Data of the Data Subject that is used by Petredec and the reason for its use.

DATA SUBJECT WITHDRAWAL OF CONSENT

This communication relates to the withdrawal of processing of all Personal Data of the Data Subject, subject to the following:

1. Data Subject completing Petredec's Data Subject Consent Withdrawal Form; or
2. Data Subject otherwise informing Petredec that it no longer consents to the processing of its Personal Data by Petredec.

PURPOSE SPECIFICATION OF PERSONAL DATA

Any Personal Data supplied by a Data Subject shall only be collected and used by Petredec for the purpose for which it was originally intended, in accordance with Data Protection Principles. In the event that the Personal Data will be used for another purpose, consent from the Data Subject will be obtained prior to the use of such information.

DIRECT MARKETING

1. Direct Marketing consists of any promotional, publicity or communications activity sent directly to particular individuals or businesses intended to promote the business' products and services.
2. Petredec is subject to certain rules and privacy laws when engaging in direct marketing to our customers and prospective customers (for example when sending marketing emails or making telephone sales calls).

USE DIRECT MARKETING

1. Petredec uses e-mail and e-marketing to send information directly to its business clients and contacts including insights, event invitations and news on products and services ("Centralised Communications.")
2. This information is not sent automatically, and you are not obliged to receive it. Petredec operates an "Opt-in" Policy for its Direct Marketing. This means you will only be sent and receive Centralised Communications if you are a client of Petredec or where we have your express consent to do so. We also reserve the right to e-mail you with Centralised Communications if you fall outside of the groups specified above, if we believe it is in your business interest to receive the communication.
3. Petredec only uses e-mail to conduct direct marketing. It does not use text messaging, telesales, post or fax to carry out direct marketing.
4. We may occasionally share Personal Data with trusted Third Parties to help us deliver efficient and quality services. Any such recipients will be contractually bound to safeguard the data we entrust in them and will not contact you to offer services.

DIRECT MARKETING TO BE RECEIVED FROM PETREDEC

1. We will use and process your data to send you Centralised Communications about:

    - Events, including invitations to seminars/webinars and/or networking events;
    - Insights, relating to the topics which you have indicated are of interest to you as part of the opt-in process, or those we deem are in your interest to receive;
    - New products or services;
    - News and information about Petredec.

2. As part of our opt-in process, you will be invited to select the service areas and sectors on which you wish to receive Centralised Communications (there is no limit to the number of topics you can select as preferences).
3. We may send you details of our products or services that we have identified as likely to be of interest to you, based on the preferences you have indicated to us.

CIRCUMSTANCES WHERE DIRECT MARKETING WILL BE RECEIVED

1. You will only receive Centralised Communications from Petredec, including information about our products and services, relevant Insights, seminar, webinar and event invitations and other news/announcements, if you are a client of Petredec, or associated with a client of Petredec, or you have opted-in to receive these communications, or we believe it is in your business interest to receive the communication.

2. You will be invited by e-mail to opt-in online as a result of:
    - you or your employer becoming a client of Petredec;
    - your attendance at an event, seminar or webinar hosted, or co-hosted, by or with Petredec;
    - your attendance at a 'public' event organised or co-hosted by Petredec;
    - you providing a business card directly to an employee of Petredec, at for example, a trade or networking / business event;
    - you registering your contact details in order to obtain information or free downloads from Petredec's website;
    - an e-mail request from you to attend an event we have advertised via social media or on our website or via a Third Party;
    - an employee adding your details to our database due to an existing relationship.

3. We record your opt-in and marketing preferences using e-marketing software, including the date and time you opted in.

4. We do not buy lists from Third Parties to use for direct marketing, unless we have proof that the Third Party has obtained opt-ins or consents within the last six months which specifically name us.

REFUSAL OF RECEIVING DIRECT MARKETING INFORMATION

1. If you would like to withdraw your consent or opt-out of receiving any Centralised Communications, you can do so using our Unsubscribe Notice.
2. Alternatively, you can also access our online preference management centre at any time where you can alter your preferences.

REPORTING A PERSONAL DATA BREACH

Petredec may be required to notify any Personal Data Breach to the data protection authority in the relevant jurisdiction and, in certain instances, the Data Subject. We have in place procedures to deal with any suspected Personal Data Breach and will notify the Data Subject or any applicable regulator where we are legally required to do so.

Where a Company Personnel knows or suspects that a Personal Data Breach has occurred, Company Personnel should not attempt to investigate the matter themselves. Immediately contact the DPO, and within the applicable legal timeframe (where relevant). You should preserve all evidence relating to the potential Personal Data Breach.

When a Personal Data Breach is reported, the following details should be provided (where possible):

(a) General nature of the security incident;
(b) General classification of people involved in the security incident, (such as external client or privileged employee);
(c) Computer systems involved in the security incident;
(d) Details of the security incident;
(e) Impact of the security incident;
(f) Possible courses of action to prevent a repetition of the security incident.

TRANSFER LIMITATION

The level of data protection afforded to individuals must not be undermined due to a data transfer. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

Company Personnel must comply with the Company's guidelines on cross-border data transfers, in particular when Personal Data is transferred outside of the UK or EU, in accordance with Data Protection Principles.

CONDITIONS FOR TRANSFER

Company Personnel may only transfer Personal Data if one of the following conditions applies:

(a) the destination country is a Member State of the EU;
(b) the EU has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;
(c) appropriate safeguards are in place such as standard contractual clauses approved for use in the EU, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
(d) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
(e) the transfer is necessary for one of the following reasons:
    i. the performance of a contract between us and the Data Subject;
    ii. reasons of public interest;
    iii. to establish, exercise or defend legal claims;
    iv. to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and
    v. in some limited cases, for our legitimate interest (provided this is confirmed by the DPO).

THIRD PARTY DATA OPERATORS

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place, to ensure conformance with Data Protection Principles.

APPLICABILITY

Petredec will only share the Personal Data it holds with another employee, agent or representative of its group (which includes our subsidiaries and its ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions

Petredec will only share the Personal Data we hold with third parties, such as its service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;
(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;
(c) the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;
(d) the transfer complies with any applicable cross-border transfer restrictions and local law requirements; and
(e) a fully executed written contract has been obtained that contains standard protective clauses which the DPO (and/or legal counsel) has approved (a “Data Processing Agreement”).

THIRD PARTY SERVICE PROVIDER DUTIES

The third party shall agree in the Data Processing Agreement to the following:

- to only use and disclose the Personal Data in accordance with Petredec’s specific written instructions;
- to take reasonable and appropriate, organisational and technical security measures to protect Personal Data supplied by Petredec or otherwise made available to the third party;
- to permit Petredec to audit the third party in terms of its compliance with relevant local laws; and
- to comply with requests by Petredec for access to the relevant Personal Data following the receipt of a valid and approved data subject request.
- The third party is not permitted to sub-contract any of the processing of the Personal Data supplied by Petredec or otherwise made available to the third party without first:
- ensuring the sub-contractor will be compliant with the relevant local law requirements; and
- obtaining prior written permission of Petredec.

The third party also agrees to co-operate with any action required to fulfill the requests or demands of any data protection authority, whether directly by such data protection authority or indirectly by Petredec.

RIGHTS OF PETREDEC

An audit of the compliance of the third party with relevant local laws to be conducted by Petredec or its authorised agent may include but is not limited to:

- ensuring that the third party transfers data securely;
- ensuring that the third party reports any security breaches or other problems to Petredec; and
- in any other way fulfill the duties of Petredec.

VARIATION OF CONTRACT TERMS

It is the duty of Petredec to monitor any changes to relevant local laws and associated regulations, and to ensure ongoing compliance with them. This may require amendments from time to time of the Data Processing Agreement.

TERMINATION OF DATA PROCESSING AGREEMENT

In terms of processing of Personal Data:

- Where the third party is found by a data protection authority to have not fulfilled its obligations in terms of compliance with relevant local laws, Petredec has the right to cancel the Data Processing Agreement with the third party with immediate effect.
- Whether for fault or any other termination reason, the third party must return or effectively destroy all Personal Data processed on behalf of Petredec without delay, unless it is required to retain such Records in terms of other legislation or regulations.

CHANGES TO POLICY

Petredec keeps this Data Protection Policy under regular review. Historic versions are available from the DPO.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where Petredec operates, which may necessitate a departure from these rules. Certain countries may have localised variances to this Data Protection Policy which are available on request to the DPO.

DPO CONTACT DETAILS

Please refer to DPO Contact information link below

https://petredec.com/dpo-contact-information