

PNL GDPR Privacy Notice

2018



 www.pnlaccounting.co.uk
 office@pnlaccounting.co.uk
 (01445) 712 409
 Strath Bay House
Gairloch
Ross-Shire
IV21 2BP





PNL GDPR Privacy Notice

We confirm that we will comply with the provisions of the GDPR and the Data Protection Act 2018 when processing personal data about you and that we have appropriate security measures in place.

We will process your personal data in order to provide you with the services you have requested and to comply with our legal and regulatory obligations. We obtain this personal data from yourself or other regulatory bodies.

In order to carry out the terms of our engagement you need to sign the Consent Form and understand that failure to do so will negatively impact the services we provide.

We will also process your personal data for management and analysis purposes.

Any of your personal data which we hold will be stored securely on our systems for a period of time defined by our internal data retention policies. Generally, this will be for the duration of our engagement with you and thereafter for as long as is required by the law.

The latest version of this Privacy Notice will be always available on our website or if you request in writing by email or letter.

Your personal data may be processed by third parties who are only permitted to use your data for specified purposes and in accordance with our instructions. Those third parties have appropriate security measures in place regarding your personal data which are in line with our policies and the GDPR legislation.

Unless you inform us not to do so in writing by email or letter, we may contact you occasionally by post or e-mail to tell you about products or services which may be relevant to you.

You have the right to apply for a copy of the information we hold about you; to have any inaccuracies corrected; and restrict processing of it. In certain circumstances you have the right to have your personal data erased, subject to legal and regulatory compliance and crime prevention. You have the right to data portability: to obtain a copy of the data you have provided to us, held digitally, in a form that allows you to transfer it to another data controller. You have the right to complain about the processing of your personal data and in the first instance please send any concerns you have, in writing, by email or letter and we will do our best to help you. If you are still unsatisfied, you have the right to complain to the Information Commissioner's Office. Contact details can be found at www.ico.org.uk.



Table of Contents *(Use the 'Ctrl'+Click' button on the required section below for further detail)*

CLIENT DATA.....	4
DATA PROTECTOR OFFICER (DPO)	4
STAFF TRAINING.....	4
HOW WE COLLECT DATA.....	4
HOW WE USE DATA.....	5
HOW WE SECURE ELECTRONIC DATA.....	5
HOW LONG WE KEEP DATA	5
RIGHT TO BE INFORMED.....	5
RIGHT TO ACCESS TO INFORMATION	5
RIGHT TO RECTIFY THE INFORMATION.....	6
RIGHT TO ERASURE	6
RIGHT TO RESTRICT PROCESSING	6
PROFESSIONAL CLEARANCE	6
DATA BREACH	6



Client Data

We only request relevant data for the services we will provide.

To comply with Anti-Money Laundering (AML) Regulations, we are obliged to hold a copy of a valid photo ID (usually passport or driving licence) and proof of address for the last 3 years for each client. This information is used to carry out an electronic ID check to satisfy AML requirements and is kept for that purpose only.

We will NEVER request *sensitive data* from our clients as:

- Race or ethnic origin
- Religious and philosophical beliefs
- Political opinions
- Physical or mental health
- Gender or sex life
- Genetic and biometric data
- Trade Union activities
- Details of criminal offences
- Children's names and information

Data Protector Officer (DPO)

We **do not**:

- carry out online profiling,
- carry out business overseas, and
- deal with sensitive info or any special data processing

Therefore we are not required to nominate a DPO but if you have any queries or concerns about your data, please get in touch with Peter Saggars (peter@pnlaccounting.co.uk) or Lynsay MacKenzie (lynsay@pnlaccounting.co.uk).

Staff Training

Before starting employment with PNL and gaining access to any personal data, staff are required to be GDPR certified and sign a confidentiality agreement

How we collect Data

We only collect data given freely from the client themselves when engaging.

If they decide not to become a client, after signing the consent, a withdrawal must be also signed and all personal information will be destroyed

When acting as an agent, dealing with HMRC matters on your behalf, there may be instances where HMRC reference numbers etc are issued directly to us as part of the registration process for a new HMRC service. In such cases, we will inform the client of any new information relating to their HMRC records, as soon as possible.

We will NEVER collect client's data from other clients or use any marketing service, unless express consent is provided.



How we use Data

We store our clients' data on our server to which only the staff is permitted to access. In accordance with our IT Support Agreement, when given our authority to do so, our IT support provider is also permitted to access our server for IT maintenance and support purposes only.

All access passwords are modified immediately once a staff member's employment with the company has ended.

We will disclose clients' data to selected, GDPR-compliant, third parties only, in order to meet HMRC regulations, the terms of our engagement or for internal administrative purposes. A list of the aforementioned third parties and how clients' data is used by them is available on request, in writing.

How we secure electronic data

Our Wi-Fi network is secured using WPA2 encryption. Our Anti-Virus system is configured to automatically update, scan emails and check for malicious websites, in compliance with the Government [Cyber Essentials Scheme](#). Password policies are in place and compliant with Cyber Essentials.

How long we keep data

Once a client's engagement with PNL ends or if a client withdraws their consent form, all data shared with third parties will be removed.

By law, we are required to hold a client's data for 7 years after which time, it will be destroyed unless the client requests otherwise, in writing.

Right to be Informed

The latest version of this GDPR Privacy Notice will be always available on our website.

All clients are strongly recommended to read it thoroughly and understand the content before signing the consent form.

If there are any questions or concerns we are happy to provide further reassurance on how we collect, use, process and delete data.

Right to Access to Information

During the engagement, the client can request any of their personal data held by us at any time, including the correspondence between our parties and any information our third parties hold for the client.

Although we will do our utmost to reply within a few days, we allow one month to comply with the request or up to three months if we acknowledge receipt of the request within the first month.

Once the engagement with a client ends and consent is terminated, only the regulated data can be provided when a request is made and we reserve the right to charge a fee to restore such data from our archive.



Right to Rectify the Information

We will always do our best to keep all data up to date on our server and with all third party softwares. If it comes to our attention that the client data is inaccurate or incomplete we will rectify immediately.

Right to Erasure

Also known as the Right to Withdraw Consent, Opt-Out or Right to be Forgotten.

If at any time the client wishes to withdraw their consent, it should be done so in writing, by email to office@pnlaccounting.co.uk or letter to the address below.

When consent is withdrawn, the client's data will be removed from all third parties within 48 hours.

We reserve the right to refuse a request for erasure, should the data be required as evidence, in the event of litigation against us.

Right to Restrict Processing

Clients have the right to 'block' or suppress the processing of personal data. In such cases, we are permitted to store the data but not continue to process it. We will retain the minimum level of information about the client to ensure the restriction is respected in future.

Professional Clearance

All new clients joining us must sign an agreement to allow us to request personal data from their previous accountant.

All clients leaving us must sign a disengagement agreement where they authorise us, in writing, to forward the personal data to the new accountant.

Data Breach

The GDPR defines a breach of security as one which 'leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

A breach can take many forms: from a person entering the office and accessing or taking personal data, to a cyber attack. Also a misplaced laptop or USB memory stick can be regarded as data breach. All data breaches (in the office or by third parties) that might compromise a client's safety will immediately be reported to the supervising authority (ICO – Information Commissioner's Office) and all affected clients will be contacted not later than 72 hours after the breach.

Notification of the breach will include:

- Nature of breach
- Date and time if known
- Likely consequences
- Proposed measures to mitigate adverse effects

All measures to ensure safety of the information will be taken.