Privacy Notice

Xeinadin Limited (Ireland)

1. Who We Are

Xeinadin Limited
Building 1, Swift Square
Northwood Park
Dublin 9, D09 A0E4
Company No. 634393

Email: data.protection@xeinadin.com

Xeinadin Limited processes personal data in accordance with the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 and applicable ePrivacy laws.

2. Our Role as Controller and Processor

Data Controller: We act as a data controller where we determine the purposes and means of processing personal data. This includes the provision of:

- Accountancy services
- Tax advisory and compliance services
- Business advisory services
- Direct services to sole traders, directors and individual clients

In these cases, we are responsible for ensuring compliance with data protection law.

Data Processor: We act as a data processor where we process personal data strictly on behalf of a client and under their instructions.

This includes services such as:

- Payroll processing
- Bookkeeping performed under client instruction
- Administrative services where the client determines the purpose of processing

In these circumstances the client (for example, the employer) is the data controller.

We process personal data under a written Data Processing Agreement in accordance with Article 28 GDPR.

Individuals whose data we process (e.g. employees) should refer to their employer's privacy notice.

We apply appropriate technical and organisational security measures in both roles.

3. Categories of Personal Data

Depending on the services provided, we may process:

- Identity and Contact Information
- Name, address, email address, telephone number
- PPSN or other government identifiers (where legally required)
- Financial and Tax Information
- Bank details
- Payroll data
- Tax returns and supporting documentation
- Accounting records and financial statements
- Income and expenditure information
- Compliance and Verification Data
- Identification documents for AML/KYC purposes
- Due diligence information
- Information required under the Criminal Justice (Money Laundering and Terrorist Financing) Acts
- Website and Marketing Data
- IP address
- Device and browser information
- Cookie identifiers
- Website usage data

We only process personal data that is necessary for the relevant service or legal requirement.

4. Lawful Basis for Processing

We rely on one or more of the following lawful bases under Article 6 GDPR:

- **Performance of a Contract Article 6(1)(b)**
  We process personal data where necessary to fulfil our contractual obligations in providing accountancy, tax, advisory or payroll services requested by our clients. Without this information, we would be unable to deliver the agreed services.

- **Compliance with Legal Obligations Article 6(1)(c)**
  We are required to process certain personal data to comply with Irish law, including:
  - Revenue record-keeping requirements
  - The Criminal Justice (Money Laundering and Terrorist Financing) Acts
  - Companies Act obligations
  - Regulatory reporting requirements

Where criminal offence data is processed, it is limited to compliance with anti-money laundering legislation and handled in accordance with the Data Protection Act 2018.

- **Legitimate Interests Article 6(1)(f)**
  We process personal data where necessary for our legitimate business interests, provided these interests are not overridden by your rights. These interests include:
  - Managing client relationships
  - Maintaining IT security and preventing fraud
  - Internal administration and risk management
  - Improving our services
  - Limited marketing to business contacts

  Where we rely on legitimate interests, we carry out an assessment to ensure that the processing is necessary and that your rights and freedoms are not overridden. You have the right to object to such processing.

- **Consent Article 6(1)(a)**
  We rely on consent where required, including:
  - Sending marketing communications (where required under ePrivacy rules)
  - Using non-essential cookies
  - Certain advertising activities

  You may withdraw consent at any time.

5. How We Collect Personal Data

We collect personal data:

- Directly from you
- From employers or authorised representatives
- Through secure client portals
- From Revenue, regulatory bodies or other public authorities where required
- From third parties for compliance purposes, including identity verification and anti-money laundering screening providers
- Through website interactions and cookies

Anti-Money Laundering (AML) Screening
To comply with our obligations under the Criminal Justice (Money Laundering and Terrorist Financing) Acts, we may obtain personal data from third-party identity verification and compliance screening providers. This may include verification of identity, sanctions screening, politically exposed person (PEP) checks and other due diligence information.

This processing is carried out to meet our legal obligations and may involve obtaining information from publicly available sources or authorised compliance databases.

6. Who We Share Data With

We may share personal data with:

- Revenue Commissioners
- Banks and financial institutions
- Accounting and payroll software providers (such as Xero, Sage, QuickBooks, BrightPay)
- Credit reference agencies where required
- Professional advisers and insurers
- Regulators or law enforcement authorities where legally required
- We may contact you by email, telephone or SMS to remind you of outstanding balances. These communications are service-related and not marketing. We may use third-party communication providers to send such reminders on our behalf.
- Where payment remains outstanding, we may also share relevant personal data with regulated firms of solicitors to recover unpaid fees or enforce contractual rights. This processing is based on our legitimate interests under Article 6(1)(f) GDPR and, where applicable, for the establishment, exercise or defence of legal claims.

Where third parties process personal data on our behalf, they are subject to written contractual obligations to process personal data only in accordance with our instructions and to implement appropriate technical and organisational security measures.

Where third parties act as independent data controllers (such as Revenue or financial institutions), they are responsible for complying with their own data protection obligations.

7. International Transfers

Some of our service providers may be located outside the European Economic Area (EEA).

Where personal data is transferred outside the EEA, we rely on European Commission Standard Contractual Clauses or other approved safeguards. We conduct transfer risk assessments where required to evaluate whether the destination country provides an essentially equivalent level of protection and implement supplementary measures where necessary.

Further information about international transfers and safeguards is available on request.

8. Data Retention

Client records are generally retained for six years from the end of the relevant accounting period in line with Irish Revenue requirements.

Longer retention may apply:

- Where required under anti-money laundering legislation
- For legal claims or dispute resolution
- For estate planning or long-term capital transactions where strictly necessary
- For legal, tax or regulatory purposes where strictly necessary

Where we act as a data processor (for example in payroll services), retention is determined by our client's instructions and applicable legal requirements.

Data is securely deleted or anonymised once retention periods expire.

9. Data Security

We implement appropriate technical and organisational measures to protect personal data, including:

- Access controls
- Secure cloud infrastructure
- Encryption where appropriate
- Confidentiality obligations for staff

In the event of a notifiable personal data breach, we will comply with reporting obligations under GDPR.

10. Your Rights

Under data protection law, you have the right to:

- Access your personal data
- Rectify inaccurate data
- Request erasure (subject to legal obligations)
- Restrict processing
- Object to processing based on legitimate interests
- Data portability
- Withdraw consent (where applicable)
- Lodge a complaint with the Data Protection Commission

To exercise your rights contact: data.protection@xeinadin.com

We will respond within one month, subject to statutory limits.

You also have the right to lodge a complaint with:

The Data Protection Commission
21 Fitzwilliam Square South
Dublin 2

www.dataprotection.ie

11. Cookies, Analytics and Advertising

We use cookies to improve website functionality and performance.

Google Analytics collects device and usage data, including IP address information, to analyse website performance.

We may use hashed contact information to create advertising audiences through Google Ads. This processing is based on our legitimate interests. You have the right to object at any time.

Advertising cookies are only used where you have provided consent.

Further details are available in our Cookie Policy.