PCI Pal Global Recruitment Data Protection Notice

Effective Date: 23rd January 2026**, Version** 1.0

1. Introduction and Contact Information

PCI Pal (referred to as "we" "our" and "us") is committed to protecting the privacy and security of your personal data and we have developed this recruitment data protection notice ("notice") to inform you of the personal data we collect, what we do with your personal data, what we do to keep it secure as well as the Rights you have over your personal data.

Throughout this notice we refer to global data protection legislation which includes:

- The UK GDPR, Data Protection Act 2018, PECR and Data (Use and Access) Act 2025
- The EU GDPR and e-Privacy Directive
- Canadian PIPEDA 2014
- Australian Federal Privacy Act 1988 and Australian Privacy Principles
- American Federal and State Privacy laws as applicable

The above also includes any new or replacement legislation which may come into force from time to time.

PCI Pal is a data controller where we have determined the purposes of why personal data should be collected and processed for recruitment purposes.

We are registered with the Information Commissioners Office (the ICO) with registration numbers ZA202963 and Z7602903.

You can contact any one of our global offices using our details included in our contact us sub-page. We have appointed an **external Data Protection Officer** (DPO) and their details are as follows:

Name: RA Data Protection Ltd
Website: https://radataprotection.com/
Email: ravi@radataprotection.com

We have also appointed an **EU GDPR Representative** called Saltire Data Protection Services Limited and are based in Ireland. If you would like to contact our EU GDPR Representatives you can do so by clicking this link and following instructions.

Our **Lead EU Supervisory Authority** is the Irish Data Protection Commission link

You can also use the above contact information to raise or discuss any data protection matters, complaints and/or concerns.

2. Legal Basis for Data Processing

The legal bases for us to process recruitment candidate data is based on:

- Contractual obligation
- Legal obligation
- Our legitimate interests

We do not request consent however if we receive a request to delete candidate information we will be happy to respond to such requests where possible.

3. Data Subjects

For our recruitment process we may process the personal data of the following individuals ("data subjects"):

- Enquirers
- Applicants
- Past unsuccessful applicants

4. Personal Data Collection

We advertise roles on our careers website and on LinkedIn. When you apply to a role our head office recruitment team in the UK will receive a notification informing them of an application. The recruitment teams will be able to review data of applicants which can include (and not limited to) the following sets of personal data:

- Name
- Contact details
- Position applied for
- Information within your CV
- Answers to any application questions
- Any tests or presentations undertaken

There may be instances of where we may need to process special category personal data (for example health information) to help us make any reasonable adjustments for interviews. Please note that we do not request this information as part of our standard process. This data will also be held for as long as necessary in line with our data retention schedules.

We strongly encourage applicants to not send through any documents such as ID documents (e.g. passport scans) or copies of certifications (unless specifically requested) as they may not be necessary and may be deleted unless requested.

Please also note applications made will enable our recruitment team to view your social media profiles such as your LinkedIn profile, and view information not included on your CV.

5. How We Obtain Personal Data

During our recruitment process we may obtain personal data about candidates through various means, which include (but is not limited to):

- Directly from the candidate
- Candidate's social media profile (e.g. LinkedIn profile)
- Specified referees
- Employee referrals
- From third-party recruitment websites

6. How Is Your Personal Data Used?

Personal data processed as part of the recruitment and onboarding process can include the following activities:

- To assess your skills, qualifications, and suitability for the role
- Carry out background and reference checks, where applicable

- Communicate with you about the recruitment process
- Keep records related to our hiring processes
- Comply with legal or regulatory requirements
- If successful offer suitable candidates' contracts of employment

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history) we will not be able to process your application successfully.

7. Criminal Conviction and Offences Data

As part of our recruitment process we carry out basic DBS checks on any new employees. We utilise a third party provider to carry out these criminal background checks on our behalf who will contact the new employee to begin the process, and we retain the DBS check data in line with our retention schedules. For more information you can contact us using our information above.

8. Background Checks

We carry out background checks (employment and right to work) with candidates as a condition of employment.

The personal data collected and processed will include (but is not limited to):

- Name
- Contact details
- Employment history
- Right to work documents
- ID (for example, drivers license, passport, etc)

For more information you can contact using our details as mentioned above.

9. Third-Parties Who We May Share Personal Data With

We do not rent, sell or purchase any recruitment related personal data to and from other organisations.

Please note there may also be instances where we may need to share personal data with a competent law enforcement body, regulatory body, government agency, court, or other third party where we believe disclosure is necessary (i) as a matter of applicable law or regulation or (ii) to exercise, establish or defend our legal rights.

10. Global Data Transfers

Our global recruitment team is based in the UK. . This means the People team may receive recruitment related data from other global locations to help fulfil any specific vacancies that may arise (i.e. intra-group data sharing). We do not transfer any recruitment data from the UK to any other third party in the EU/EEA, in a adequate listed country or third countries who may not have strict and similar data protection laws to the UK. For more information you can contract us using our details above.

11. Data Retention

We will retain recruitment related personal data for as long as necessary in line with various requirements, such as for example, best practice recommendations (e.g. ICO recommendations), relevant guidelines (e.g. ACAS guidance) or for as long as mandated under specific legislation (e.g. Equality Act 2010). We will also determine appropriate retention periods based on our legitimate interests where identified. This includes both data controller and joint-data controller retention periods.

At the end of the retention period personal data will be securely deleted

12. Data Security

We have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to employees and other third parties who have valid business reasons to access this data. They will only process your personal data on our instructions and they are subject to a duty of confidentiality. If we become aware of any loss, misuse, alteration of personal data we will investigate the incident at hand and report (when needed to relevant parties) such instances.

13. Data Subject Rights

Under data protection legislation individuals have the following rights:

1. Right to be informed
2. Right to access personal data
3. Right to rectify personal data
4. Right to erase personal data
5. Right to object to personal data
6. Right to have data ported
7. Right to restrict personal data
8. Right to not have personal data processed by automated means and profiled

If you would like to exercise any of the above Rights you can do so by sending a written request using details above. Please note we may ask for ID (e.g. passport scan, drivers license etc) to verify identity where needed. Upon successful verification, and where appropriate, we will delete and remove all copies of ID received.

Should we also require extension of time to help fulfil any Right requests, we will contact requestors as soon as possible with reason(s) why an extension is needed and when Right requests can be fully carried out and completed.

14. Concerns and Complaints

If you have any concerns and/or complaints to this privacy notice and/or to how we process personal data please contact us using our details above.
You can make a complaint to data protection authorities at any time however we hope that you would consider raising any issue or complaint you have with us first. Below is a list of authorities and contact links:

- UK ICO link.
- Irish Data Protection Commission link
- Australian Office of the Australian Information Commissioner link
- Office of the Privacy Commissioner of Canada (English) link
- US North Carolina Department for Information Technology link

We will check these links for updates and amendments from time to time.

15. Recruitment Privacy Notice Updates

We will review this notice and make changes to it from time to time. We recommend that you check this notice to see where changes have been made and to ensure you are able to review updated information at all times.