

OEL NATIONWIDE PERSONNEL LIMITED

Company Registration Number: 15538543

Registered Office: 102 Stamshaw Road, Portsmouth, England, PO2 8LU

Information Security and Data Protection Policy (GDPR)

Ref: PL/007 | Version 2 | Reviewed: May 2026

Data Protection Officer: Julie Siva (Compliance Manager)

1. Introduction and Purpose

OEL Nationwide Personnel Limited processes personal data in relation to its own staff, work seekers and individual client contacts. It is vitally important that we abide by the principles of the General Data Protection Regulation (GDPR) 2018 and, where applicable, EU GDPR requirements.

This policy applies to all personal data processed by OEL Nationwide Personnel Limited, including data relating to candidates recruited for domestic and international programmes. As a UK-based organisation that may process personal data relating to individuals located in EU member states, OEL ensures that all data is collected, stored and transferred in compliance with applicable data protection legislation, including cross-border transfer requirements.

2. Scope

This policy applies to:

- All employees, contractors and recruiters working on behalf of OEL Nationwide Personnel Limited
- All personal data processed in connection with work-finding services, including data relating to candidates in the United Kingdom and internationally
- All data shared with third-party clients, including where candidates are to be employed by an overseas operating company
- International recruitment programmes, including those operating within the European Economic Area (EEA)

3. Data Protection Principles

OEL Nationwide Personnel Limited, as data controller, shall

ensure that all personal data is:

- Processed fairly, lawfully and transparently
- Collected only for specified, explicit and legitimate purposes, and not processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Retained for no longer than is necessary for the purpose for which it is processed
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

4. Lawful Basis for Processing

Personal data will only be processed where a lawful basis exists. For work-seeking candidates, the primary lawful basis is consent. By instructing OEL Nationwide Personnel Limited to find work and providing personal data contained in a CV or application, candidates give their consent to processing their details for work-finding purposes.

Where data is intended to be processed for any other purpose, OEL Nationwide Personnel Limited must obtain specific consent from the individual concerned.

5. Data Retention

OEL Nationwide Personnel Limited will not retain personal data for longer than is necessary for the purpose for which it was collected. The following retention periods apply:

- Active candidates: data retained for the duration of the recruitment process and for a period of 12 months following the conclusion of the programme or candidate withdrawal
- Placed candidates: data retained for a period of 6 years following the end of the placement, in line with legal and contractual obligations
- Unsuccessful candidates: data retained for a maximum of 6 months following the conclusion of the recruitment process, unless the candidate has consented to a longer retention period for future opportunities
- Compliance documentation (licence verification, police certificates, right to work): retained in line with client

contractual requirements and applicable regulatory obligations, and no longer than 6 years

At the end of the applicable retention period, personal data will be securely deleted or anonymised. Destroying or disposing of personal data counts as processing and must be carried out appropriately, including secure shredding of physical documents.

6. Cross-Border Data Transfers

Where OEL Nationwide Personnel Limited processes personal data relating to individuals located in EU member states, or transfers personal data from the UK to countries within the EEA or beyond, appropriate safeguards will be put in place to ensure compliance with both UK GDPR and EU GDPR cross-border transfer requirements.

For international recruitment programmes, including those based in Germany or other EU member states:

- Candidate personal data will be collected and processed in the UK under UK GDPR
- Data shared with EU-based client organisations will be limited to what is strictly necessary for hiring decisions
- OEL will ensure that any transfer of personal data to EU-based operating companies is conducted under appropriate legal mechanisms, including standard contractual clauses where required
- Candidates will be informed at the point of data collection that their personal data may be shared with an overseas employer as part of the recruitment process

OEL Nationwide Personnel Limited will endeavour to ensure that personal data is not transferred to countries outside of the EEA without adequate protection being in place.

7. Individual Rights

Individuals hold the following rights under UK GDPR and EU GDPR:

- The right to be informed about how their data is used
- The right of access to their personal data
- The right to rectification of inaccurate data
- The right to erasure ('right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object to processing
- Rights in relation to automated decision making and

profiling

Any requests to exercise these rights should be directed to the Data Protection Officer, Julie Bhalla, at office@oelnp.com. Requests will be acknowledged within 72 hours and responded to within one calendar month.

Any requests for access to a reference given by a third party must be referred to the Managing Director and treated with caution, as the person writing the reference also holds rights under data protection legislation.

8. Data Security

OEL Nationwide Personnel Limited applies the following general security principles to ensure the confidentiality, integrity and availability of all personal data held:

- Personal data may only be accessed, altered, disclosed or deleted by those authorised to do so
- Computer screens must not be left open and unattended by individuals who have access to personal data
- Passwords must not be disclosed or shared
- Email must be used with care when transmitting personal data
- Personnel files and personal data must be stored securely and not removed from their usual place of storage without good reason
- Personnel files must be locked away when not in use
- Care must be taken when sending personal data in internal or external correspondence
- Any breach of security must be treated as a disciplinary issue and reported to the Data Protection Officer immediately

The incorrect processing of personal data — including sending an individual's details to the wrong person, allowing unauthorised access, or processing data for purposes for which consent was not given — may give rise to a breach of contract and/or negligence claim. A failure to observe this policy will be treated as a disciplinary offence.

9. Data Breach Procedure

In the event of a personal data breach, OEL Nationwide Personnel Limited will:

- Notify the Data Protection Officer immediately upon becoming aware of the breach
- Assess the risk to individuals affected

- Where the breach is likely to result in a risk to individuals, notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware
- Where the breach is likely to result in a high risk to individuals, notify those individuals without undue delay
- Document all breaches, regardless of whether notification to the ICO is required

10. Data Protection Officer

OEL Nationwide Personnel Limited has designated Julie Bhalla (Compliance Manager) as its Data Protection Officer. Julie is responsible for:

- Overseeing compliance with this policy and applicable data protection legislation
- Acting as the point of contact for individuals wishing to exercise their data protection rights
- Monitoring data protection compliance across all recruitment programmes, including international projects
- Liaising with the ICO and relevant supervisory authorities where required
- Ensuring this policy is reviewed and updated at least annually

Julie Bhalla can be contacted at: office@oelnp.com

11. Human Rights

In dealing with personal data, OEL Nationwide Personnel Limited will at all times respect the following rights under the Human Rights Act 1998:

- Right to respect for private and family life [Article 8]
- Freedom of thought, conscience and religion [Article 9]
- Freedom of expression [Article 10]
- Freedom of assembly and association [Article 11]
- Freedom from discrimination [Article 14]

12. Policy Review

This policy will be reviewed annually as a minimum, or sooner where there is a material change in data protection legislation, business operations, or the nature of data processed by OEL Nationwide Personnel Limited.

Signed: *Narcis Petaca*

Name: Narcis-Valentin Petaca

Title: Managing Director

Date: May 2026

Data Protection Officer: Julie Siva

Version: 2 | Supersedes: Version 1 (June 2024)

Document Reference: PL/007