# Privacy Policy

Staffline Recruitment Limited (03996086), Datum RPO Limited (07741572), Brightwork Limited (SC296104), Driving Plus Limited (02436612) and Staffline Group Plc (05268636) and its subsidiaries care about your privacy and are committed to processing your personal information in accordance with fair information practices and applicable data privacy laws (specifically, the UK General Data Protection Regulation ('GDPR') and the 2018 Data Protection Act). Within this Privacy Policy, all noted companies above are referred to individually and collectively as 'the Company'.

## Scope

This notice explains how the Company handles personal information relating to employees, applicants, workers, former employees, dependants, beneficiaries, contractors, consultants and temporary agency workers in connection with its recruitment, workforce management, employment and related human resources activities. The Company may amend this notice from time to time, should it become necessary to do so.

## Collection and Use of Personal Information

The Company will process your personal information to administer the employment and/or contractual relationship with you, and it shall do this by using at least one workforce management system/platform, and any applicable/associated systems as appropriate. The Company may collect, use, and transfer your personal information through automated and/or paper-based data processing systems.

The Company has established routine processing functions (such as processing for regular payroll and benefits administration) and will also process personal information on an occasional or ad hoc basis (such as when an employee is being considered for a particular new position or in the context of changes to marital status, for example).

Where processing activity is specific to a site, client assignment or role, the Company may provide supplementary privacy information during recruitment, onboarding, induction or at the point that the relevant data is collected. In the normal course of human resources activities, the Company will collect the following types of personal information:

- Personal identification information, such as your name, home address, date of birth, gender, work-related photographs, and telephone numbers.
- Government-issued documents and/or identification numbers, such as national ID, for identification, audit, and payroll purposes.
- Immigration, right-to-work and residence status, together with copies or records of prescribed right-to-work documents, Home Office online check results, identity verification outputs and photographic identity documentation needed to carry out, evidence and audit right-to-work checks and to establish or maintain a statutory excuse and confirm your identity when attending work/assignment.
- Job-related information, such as years of service, work location, employment ID, work record, vacation absences, and contract data.
- Educational and training information, such as your educational awards, certificates and licenses, vocational records, and in-house training attendance.
- Family and emergency contact details.
- Recruitment and performance-related data, such as objectives, ratings, comments, feedback results, career history, work equipment, career and succession planning, skills and competencies and other work-related qualifications.
- CCTV footage and other information obtained through electronic means such as swipe-card records or access-control records – where applicable and proportionate to the purpose.
- Information related to your usage of the Company's assets.
- Information needed for compliance, vetting and risk management such as disciplinary records, identity verification information, employment references, screening results, background check reports, criminal record check information (where permitted by law), and security-related information relevant to the role or assignment.
- For certain roles, particularly those in regulated, client-controlled or security sensitive environments, the Company may also collect and process information relating to enhanced screening requirements, including employment history verification, address checks, qualification checks, financial probity checks where appropriate and criminal background checks, where permitted by law and necessary for the role.
- Time and attendance data processed through systems operated or selected by the Company or required by a client, including clocking, swipe-card, access-control, geolocation or other attendance-verification data where appropriate. In some operational environments this may include biometric data. Where biometric data is used to uniquely identify an individual, it is special category data and will only be processed where the Company has identified a valid lawful basis

under Article 6 UK GDPR and an additional condition under Article 9 UK GDPR and the Data Protection Act 2018, completed any required Data Protection Impact Assessment, and implemented appropriate safeguards and supplementary privacy information.

- For certain roles, the Company may process health information, occupational health assessment, fitness for work information and drug and alcohol testing results where required for safety, legal compliance, client requirements or the effective administration of the employment or contractual relationship.
- Payroll and payment or benefits-related information, such as salary and insurance information, dependents, government identifier or tax numbers, bank account details, and employment related benefits information.
- Information you choose to provide about receipt of Universal Credit or participation in relevant government employment or support initiatives. This may be used to assess eligibility for support, facilitate engagement with the Department for Work and Pensions or an authorised delivery partner, and administer available initiatives or funding. The Company will explain the relevant purpose and sharing arrangements at or before collection and not providing this information will not affect your general registration with the Company unless the information is required for a specific scheme.
- Driving and transport compliance information, where driving is required as part of an individual's role or assignment, including driving licence details, categories and entitlements, licence validity and expiry information, endorsements, penalty points, disqualifications or restrictions, and other information necessary to confirm continued entitlement and suitability to drive. This may include information obtained from the DVLA or through an authorised third-party driver compliance service and information required to meet applicable Operator's Licence, road transport, driver safety and regulatory compliance obligations.

The Company may use survey platforms from time to time to seek feedback on services, engagement and worker or employee satisfaction. Where the Company carries out profiling or uses automated processing that produces legal effects or similarly significant effects, it will do so in accordance with applicable data protection law and provide appropriate information about your rights.

The Company processes personal information for the following purposes:

- Workforce planning, recruitment, and staffing.
- Screening, vetting and right-to-work verification including enhanced checks where required for particular roles or regulated environments.
- Workplace safety, occupational health, fitness for work assessments and drug and alcohol testing where required for particular roles.
- Time and attendance management, including identity verification (imposter and unauthorised substitution prevention), attendance-verification technologies and, where justified and appropriately safeguarded, biometric systems operated by the Company or required for use on a client platform.
- Audit, assurance and investigation activities, including call recording review, complaint handling, incident investigation, and direct or indirect third-party audits undertaken for client, regulatory, accreditation, labour-supply-chain or tax-compliance purposes.
- Workforce administration, payroll, compensation, and benefit programs.
- Performance management, learning and development.
- Advancement and succession planning.
- Legal compliance, including compliance with government authority requests for information, liens, garnishments, and tax compliance.
- Workplace management, such as travel and expense programs and internal health and safety programs.
- Internal reporting.
- Audit obligations and assurance requests from external accreditation bodies, clients, client-appointed or other direct and indirect third-party auditors, HM Revenue & Customs and other competent authorities. This may include payroll, payment, deduction, tax, labour-supply-chain and supporting worker information where necessary and proportionate to assess tax compliance, or applicable joint and several liability or a reasonably identified risk of such liability.
- To protect the Company, its workforce, and the public against injury, theft, legal liability, fraud, or abuse.
- Other legal and customary business-related purposes.
- To receive, assess, negotiate and administer lawful trade union access requests and access agreements, including arrangements for physical or digital access to workers, and to communicate with workers and recognised or independent trade unions where required or permitted by law.
- To identify and facilitate access to government employment, skills, welfare-to-work or funding initiatives, including engagement with the Department for Work and Pensions or authorised delivery partners where an appropriate lawful basis and transparency arrangements are in place.
- To establish, maintain, verify or audit the Company's statutory excuse and, where extended liability may apply, to obtain and assess assurances and right-to-work evidence held by a supplier or other party in the labour supply chain.

- Driver and transport compliance, including verifying and periodically monitoring driving licence validity, entitlement to drive, endorsements, restrictions and other relevant driving-status information; assessing suitability for driving duties; protecting road and workplace safety; and complying with applicable Operator's Licence, road transport and other legal or regulatory obligations.

The Company may process special category personal data where this is necessary for employment, social security and social protection purposes, for the establishment, exercise or defence of legal claims, for reasons of substantial public interest, where permitted by law, or where another valid condition under Article 9 UK GDPR and Data Protection Act 2018 applies. Such data will only be processed where appropriate safeguards are in place and, where consent is relied upon, only where this is validly obtained.

Your personal information may be shared with a client, or a client's representative, where this is necessary to arrange, administer, monitor or conclude an assignment to verify suitability for a role, to manage attendance or performance on assignment, to meet legal or regulatory requirements, or to address complaints, incidents or audits connected with the services being provided. Depending on the role or assignment, this may include identity and right-to-work verification, assignment details, attendance information, training or competency information, screening status, occupational health or fitness-for-work status where relevant and lawful, and other information reasonably required to administer the assignment.

The Company may share personal information with a client or its authorised representative where there is a lawful basis for doing so. Each request will be assessed against its stated purpose, the recipient's authority to receive the information, and the necessity and proportionality of the disclosure. Appropriate security and privacy safeguards will apply.

Where appropriate, the Company may obtain driving and licence compliance information from third parties, including the Driver and Vehicle Licensing Agency (DVLA), authorised driver verification or compliance service providers, and other relevant regulatory or licensing bodies.

The Company may share workforce statistics or reports with clients where there is a legitimate need to do so. Where possible, this information will be provided in aggregated or anonymised form. Where personal data is required, the Company will assess the request on a case-by-case basis and only disclose what is necessary and proportionate for the stated purpose.

Where a lawful trade union access request or access agreement applies, the Company may use or disclose limited worker contact or access information, or facilitate digital communications, only to the extent required or permitted by law and the agreed or ordered access arrangements. The Company will not provide unrestricted access to workforce data and will apply data minimisation, security and access controls.

The Company may share relevant registration, Universal Credit or scheme-participation information with the Department for Work and Pensions, another competent public authority or an authorised delivery partner where necessary to assess or administer an initiative, support or funding and where an appropriate lawful basis applies.

For tax-compliance and labour-supply-chain assurance, the Company may disclose necessary and proportionate payroll, assignment, payment, deduction, tax and supporting worker information to HM Revenue & Customs, clients, professional advisers, and direct or indirect third-party audit firms. Information will be limited to what is reasonably required for the audit or for assessing applicable joint and several liability or a reasonably identified risk of such liability.

Where extended right-to-work liability may apply, the Company may request, receive, review and retain assurances, audit records, right-to-work check outputs and supporting identity or photographic evidence from a supplier, employment business or service provider to assess whether prescribed checks have been completed and evidence retained. The Company may disclose equivalent evidence where it is itself required to provide assurance within the relevant contractual chain.

The Company may obtain information about you from third party sources where relevant to the recruitment, onboarding or workforce administration. These sources may include job boards, social media platforms, referees, former employers, screening providers, occupational health providers, identity verification providers, criminal record checking bodies where applicable, and clients where relevant to an assignment or onboarding process. The Company carries out Data Protection Impact Assessments where required to assess any high-risk processing activities. This forms part of our commitment to ensuring appropriate safeguards are in place to protect personal information and to uphold the rights and freedoms of individuals, in accordance with our obligations under data protection law.

The Company uses third-party service providers to support recruitment, workforce management, payroll, screening, technology, occupational health, communications and other business operations. Where a provider acts as our processor, it may process personal information only on our documented instructions, unless otherwise required by law, and under an appropriate data processing agreement. Some providers act as independent controllers for specified activities. Where this applies, the Company will identify those activities and ensure that sharing has a lawful basis, appropriate transparency and suitable contractual arrangements. A provider is not authorised to use personal information for its own purposes merely because it has received that information from the Company.

Where personal data is transferred outside the United Kingdom, the Company will ensure that the transfer is made in accordance with applicable data protection law and that appropriate safeguards are in place. These safeguards may include adequacy regulations or approved contractual safeguards, depending on the destination and the nature of the transfer. Where appropriate, transfers may take place under UK adequacy regulations or using approved safeguards, such as the UK International Data Transfer Agreement or the UK Addendum to EU Standard Contractual clauses. You can request further information about the safeguards including how to obtain a copy where applicable by contacting the DPO team.

## Lawful Basis

The Company processes your personal data under one or more of the following lawful bases, depending on the nature of the processing:

- Performance of Contract (Article 6(1)(b))
- Compliance with a legal obligation (Article 6(1)(c))
- Legitimate interests (Article 6(1)(f))
- Consent where this is the appropriate lawful basis (Article 6(1)(a))

Where special category personal data is processed, the Company will rely on an appropriate condition under Article 9 UK GDPR and where required, the Data Protection Act 2018. Depending on the circumstances, this may include employment, social security and social protection obligations, legal claims, substantial public interest conditions, or explicit consent where this is the appropriate basis.

Where criminal offence data is processed, including criminal record check information, the Company will do so only where authorised by law, with appropriate safeguards and in accordance with Article 10 UK GDPR and the Data Protection Act 2018.

Where the Company relies on your consent, you may withdraw it at any time using the method explained when consent was obtained or by contacting DPO@staffline.co.uk. Withdrawing consent will not affect the lawfulness of processing carried out before withdrawal.

## Disclosures

The Company may disclose your personal information for its legitimate purposes or a third party's legitimate interests for the continuity of its business/service, in the following circumstances:

- Within the Company, and with clients, payroll providers, technology providers, screening and vetting providers, occupational health providers, professional advisers, insurers, auditors, regulators, public authorities, and other service providers acting on the Company's behalf where disclosure is necessary for the purpose set out in this notice.
- A newly formed, acquiring or successor organisation where the Company is involved in a merger, acquisition, sale or transfer of business.

The Company may also disclose your details to any recipient:

- With your consent, where consent is the appropriate legal basis for the disclosure.
- Where disclosure is necessary to establish, exercise or defend legal claims, to investigate incidents or complaints or to comply with legal or regulatory obligations.
- When reasonably necessary such as in the event of a life-threatening emergency.

## Choice

Where the Company relies on legitimate interest as the lawful basis for processing, you may have the right to object to that processing in certain circumstances. You also have the right to object to processing for direct marketing purposes. The Company will consider such objections in accordance with applicable data protection law.

## Automatic Processing

The Company may use automated systems and profiling tools to support recruitment, workforce administration, analytics, service improvement and related business processes. Where the Company uses solely automated decision-making that produces legal effects or similarly significant effects, it will provide additional information about that processing and the rights available to you. For information about your rights in relations to Automatic Processing, see 'Know Your Rights'.

## International Transfers

Your personal information may be transferred outside the United Kingdom where this is necessary for the purpose described in this Privacy Policy, including where systems or service providers are located overseas. Where such transfers take place, the Company will ensure that appropriate safeguards are used in accordance with applicable data protection law.

## International Access and Third-Party Platforms

In the course of providing recruitment, workforce management and compliance services, the Company may use third-party platforms and systems (including those provided by clients or service providers) which may be accessed from locations outside the United Kingdom. Where this occurs, access to personal data is limited to what is necessary for the relevant purpose and is subject to appropriate contractual, technical and organisational safeguards.

The Company ensures that any such international access or transfer complies with UK data protection law, including the use of approved transfer mechanisms and appropriate security measures.

## Accuracy

The Company takes reasonable steps to ensure that personal information is accurate, complete, and current. Please note that you have shared responsibility with regards to the accuracy of your personal information. Please notify the Company through your local site contact of any changes to your personal information or that of your beneficiaries or dependants.

## Access

You may reasonably access and update the personal information pertaining to you that is on file with the Company. You can exercise this right by contacting: DPO@staffline.co.uk

- Your ability to access and correct personal information is not limited by transfers of personal information – the ability shall exist regardless of where personal information is physically situated within the Company.
- Your right of access may be subject to exemptions and restrictions permitted by applicable data protection law. The Company will assess these individually, including where information concerns another person or is legally privileged. A request will not be refused solely because it is repeated or concerns sensitive Company information. Where the Company refuses or limits a request, it will explain the reasons, where legally permitted, and how you may challenge the decision or complain to the ICO.

## Right to Erasure

You may ask the Company to erase your personal information where the right to erasure applies under data protection law. The Company will assess your request and explain any lawful reason for retaining the information, including where retention is necessary to comply with a legal obligation or to establish, exercise or defend legal claims.

## Security

The Company takes precautions to protect personal information from loss, misuse, and unauthorised access, disclosure, alteration, and destruction. The Company has taken appropriate technical and organisational measures to protect the information systems on which your personal information is stored and require its suppliers and service providers to protect your personal information by contractual means.

## Retention

Your personal information will be retained for no longer than is necessary for the purpose for which it was collected, in accordance with the Company's retention schedule and applicable legal, regulatory, contractual and business requirements. Retention periods may vary depending on the information and purpose. Right-to-work records and supporting identity evidence will be retained in line with applicable Home Office guidance for the period needed to establish or maintain the statutory excuse, and will then be securely deleted unless a longer period is required for another lawful purpose. Further information about relevant retention periods can be made available on request.

This may include retaining recruitment, employment, payroll, screening, occupational health, incident, complaint or audit-related records for different periods, depending on the purpose and legal basis for processing.

The Company may contact you about suitable work opportunities or related services where it has a lawful basis to do so. You may opt out of non-essential communications at any time; this will not affect information that the Company must retain or communications it must issue for legal, contractual or operational reasons.

To opt out of communications about work opportunities or related services, use the opt-out method provided in the communication or contact DPO@staffline.co.uk. This will not prevent communications necessary to administer an existing assignment or employment relationship or to meet legal obligations.

## Handling Privacy Concerns

If you have any questions about this notice or if you believe that your personal information is not handled in accordance with the applicable law or this notice, you have several options:

Contact the Company

- Discuss the issue with your supervisor or another supervisor or manager.
- Contact the Company's People department (enquiries@staffline.co.uk)
- Contact the Company's Data Protection Officer (DPO@staffline.co.uk)

Contact the Information Commissioner's Office (the 'ICO')

- Telephone the ICO helpline (0303 123 1113)
- Visit the ICO website (https://ico.org.uk/global/contact-us/)
- Write to the ICO at the following postal address:
  Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

## The Company's ICO Registration Numbers are as follows:

- Staffline Recruitment Limited: Z2743868
- Brightwork Limited: Z9636732
- Datum RPO Limited: ZA895607
- Driving Plus Limited: ZB470713
- Staffline Group PLC: Z8383724

## Know Your Data Protection Rights

The UK General Data Protection Regulation (GDPR) and the 2018 Data Protection Act (DPA) enshrines a number of rights for data subjects which are listed below, all of which are supported by the Company. Further information about these rights may be accessed by clicking the link shown at the bottom of the page.

1. The right to be informed:
   *The right to be informed encompasses our obligation to provide 'fair processing information'. This emphasises the need for the Company to be transparent about how your personal data is used.*

2. The right of access:
   You have the right to request access to your personal information and ask us to correct inaccurate information.

3. The right to rectification:
   *You are entitled to have personal data rectified if it is inaccurate or incomplete.*

4. The right to erasure:
   *The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable you to request the deletion or removal of personal data where there is no compelling reason for its continued processing.*

5. The right to restrict processing:
   *Under the DPA, you have the right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar. Where processing is restricted, we will normally store the information and only use it in limited circumstances permitted by law.*

6. The right to data portability:
   *The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services. It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.*

7. The right to object:
   *You have the right to object to: (a) processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); (b) direct marketing (including profiling); and (c) processing for purposes of scientific/historical research and statistics.*

8. Rights in relation to automated decision making and profiling:
   *The GDPR provides safeguards for you against the risk that a potentially damaging decision is taken without human intervention.*

More detailed information on each of the rights can be found here: https://ico.org.uk/for-the-public/