Convergence Group's Employee Privacy Policy

This is Our Privacy Statement to let you know how we look after the personal information we hold about You as an employee of Convergence (Group Networks) Limited.

Convergence Group take your privacy seriously and aim to be open and transparent with you on how we deal with your personal information. If you have any questions in relation to this policy or about the ways that we use your personal data, we encourage you to contact our People Team. Also, please contact us if you have any concerns that this policy has not been complied with.

Our Data Protection Officer is responsible for ensuring compliance with relevant data protection legislation. If you need to contact the DPO then you can do so by emailing contact@bulletproof.co.uk

This policy covers the following points:

1. **What information we may hold about you**
2. **How will we use information about you and the legal reason for doing so**
3. **The type of third parties we might share your personal information with**
4. **How long we will keep your information for**
5. **Data Protection Impact Assessments**
6. **How you can access the information we hold about you**

1. What information we may hold about you

We may collect, store and use the following personal data about you:

- Personal contact details which may include name, gender, title, home address, work and personal email address, work and personal telephone numbers.
- Other personal details including your date of birth, marital status, photograph, salary and bank details (including any salary deductions), national insurance number, employee ID, job title, contract details and signature.
- A copy of your birth certificate, passport, driving licence, right to work permit or visa, security clearance, car registration, make and model if applicable to your role at work.
- Recruitment information (including references and other information included in a subject profile, CV or cover letter or as part of the application process). Personal information gathered during your application process, including psychometric test data and personality test data.
- Work related information, for example, qualifications and professional accreditations, employment records (including job titles, work history, working hours and training records), and professional certifications and membership records (e.g., CCIE or Prince II).
- Disciplinary details, behaviour details (particularly around health & safety and security) and work performance information.
- Emergency contact details.
- We may also hold certain data which is categorised as special data about you which may include health and medical records, criminal history, disability details, citizenship and nationality if applicable.

- Work related username, machine ID and IP address, browsing history, location and location history and compliance information.
- Subject profile if provided from a recruitment company.
- If you are involved in either a security or a health & safety incident, then the information that we gather under our obligations.
- Voice recordings from company phones. Video and voice recording from calls over the Internet (such as Microsoft Teams).
- We may also hold information relating to your children if you have opted to include them as a beneficiary of your health benefits. We will only hold information that you give to us on children and only for the purpose given, otherwise we do not hold information on children.

2. How will we use information about you and the legal reason for doing so

We process personal information to manage our contractual relationships, provide the services we offer as a business & to measure performance of our processes. We will make sure that we only process the information in the way and to the extent that we are permitted to under the current law, which includes having a legal reason for doing so. The following legal grounds are the ones which apply to the way that we use your personal information:

- Contract – where we need your personal information in order to perform the contract that we have entered into with you.
- Legitimate Interests – Where we need your personal information in pursuit of our legitimate interests in providing you employment as long as these do not override your fundamental rights and interests.
- Legal obligation – Where we need to comply with a legal obligation to which we are subject.
- Consent – Where you have provided us with your consent to process the personal information, including consent to process medical information you have given us as part of the employment process.

In particular the following legal basis apply:

- Contractual obligation - your contact, bank and work-related details are needed to fulfil our contractual obligations with you.
- Legitimate Interests - information about you, including your photograph, so that we can create an employee ID which helps to produce internal information such as directories to share with employees and those in the process of joining Convergence Group.
- Legitimate Interests (in ensuring our network is being used in line with our Acceptable Use Policy) – when we use the information to track your location history and your use of the IT systems.
- Legal obligations – when we require information to comply with legal obligations around health & safety requirements, right to work information, salary deductions and security clearance.
- Legitimate Interests (compliance to our certifications) – for carrying out security clearance or medical clearance (in line with the job role) to allow you to perform your role and maintain our contractual obligations and certifications.
- Legal obligation – if we are required to notify our insurance providers.
- Legal obligation – if we are required to inform a law enforcement or Government body.

- Legitimate interests (of maintaining our certifications) – when required to inform our regulators.
- Legitimate Interest (ensuring employee performance is meeting the quality expectations of the business and an audit trail of conversations where legal or contractual agreements may be made) – when monitoring our telephone and video conversation recordings.
- Legal obligation – when we are required to contact you if we wish to use your information for a purpose not set out in this policy.
- Consent – when you give us medical and key contact information in line with the purposes stated on the forms.

We will only use your personal information for the legal basis for which we collected it. If we reasonably consider that the basis has changed or need to use your personal information for another purpose, then we will let you know and notify you of the new legal basis.

3. The type of third parties we might share your personal information with

In order to manage our responsibilities, we use third parties for completing certain tasks, some of whom require us to share your personal information with them in order to be able to complete their obligations.

We shall ensure that any third party we use respects the security of your information, in particular that:

- They have provided appropriate safeguards in relation to the processing and transfer of the data (particularly if the transfer of data is outside of the UK);
- You have the enforceable rights available to you; and
- There is an adequate level of technical and organisational measures in place to protect to any Personal Data that is processed and transferred.

Below are the categories or functions provided by the third parties which we use:

- Employee management software tools;
- Taxation (HMRC);
- Bankers;
- Pension providers and other financial institutions;
- Occupational health providers;
- Compliance advisors and auditors;
- Fleet providers;
- Regulators and law enforcement agencies;
- Security clearance providers;
- Network providers;
- Partners or Customers (if they have specified that they require certain information regarding those visiting site due to the nature of their business or profession such as hospitals or government bodies).

If you want to know which specific third parties we pass your information to please contact us at compliance@convergencegroup.co.uk and we will pass that information to you.

4. How long we will keep your information for

We will keep your information for as long as is necessary for us to perform the purpose which we have collected it for, except where we are required to keep it for longer to fulfil our legal obligations, (then we will keep it for the time required by the law).
In particular:

- We will keep any information contained in your contract for a minimum period of 7 years after your contract has been terminated;
- We will keep any information contained in your financial records for a minimum period of 7 years;
- Any security or health and safety compliance information will be kept for 10 years; and
- IT related information is kept for no longer than 2 years past the end of your employment contract;
- Voice recordings from company phones are kept for 5 years.
- Video recordings data from Microsoft teams will be stored securely with Numonix in UK data centres, for 12 months and only accessible to authorised management.

5. Data Protection Impact Assessments

At Convergence Group we have identified data processing activities we believe could result in a high risk to the rights and freedoms of individuals. Data Protection Impact Assessments (DPIA's) have been conducted on the following processing activities we undertake as an organisation-

- The use of our CRM system where we process Customer Data.
- Health & medical information collected as part of Display Screen Equipment (DSE) Assessments and health & safety reporting.
- Processing of medical information.

DPIA's can be made available to interested parties by contacting our Compliance Team at compliance@convergencegroup.co.uk

6. Your Data Rights

In this section, we have summarised the rights that you have under General Data Protection Regulation. Some of the rights are complex, and not all the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.
Your principal rights under General Data Protection Regulation are:

- Right to Object
- Right of Access
- Right to be Informed
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability

The Right to Object
You can exercise this right if:

- Processing relies on legitimate interest
- Processing is for scientific or historical research
- Processing includes automated decision making and profiling
- Processing is for direct marketing purposes

The Right of Access

- You or any third party acting on your behalf with your authority may request a copy of the personal data we hold about you without charge.
- We will ask to verify your identity or request evidence from the third party that they are acting on your behalf before releasing any personal data we hold about you.

The Right to be Informed

- We are required, to provide clear and transparent information to you about how we process your personal data. This privacy notice addresses this right.

The Right to Rectification

- If you believe the personal data we hold about you is incorrect or incomplete you have the right to correct this and you may exercise this right along with the right to restrict processing until these corrections are made.

The Right to Erasure

- If there is no legal basis or legitimate reason for processing your personal data, you may request that we erase it.

The Right to Restrict Processing

- You may ask us to restrict the processing of your personal data. This means we will still hold it but not process it. This is a conditional right which may only be exercised when:
    - Processing is unlawful
    - We no longer need the personal data, but it is required for a legal process
    - You have exercised your right to object to processing and require processing to be halted while a decision on the request to object is made.
    - If you are exercising your right to rectification

The Right to Data Portability

- You can request that your personal data is transferred to another controller or processor in a machine-readable format if:
    - Processing is based on consent
    - Processing is by automated means (i.e. not paper based)
    - Processing is necessary for the fulfilment of a contractual obligation

The Right to Withdraw Consent

- Where you have provided your consent to us for the processing of your personal data, you can with draw this consent at any time.

For more information on your rights and how to exercise them please contact us on: Compliance@convergencegroup.co.uk

7. How you can access the information we hold about you

If You would like to access some or all of your personal information, please email compliance@convergencegroup.co.uk or write to the People Team at our head office.
If you send us your request electronically, where possible we will provide the information to you electronically.

If you have any complaints relating to your personal information that is held or processed by Convergence Group, please email compliance@convergencegroup.co.uk in the first instance. Convergence Group retain an outsourced Data Protection Officer (DPO), If you wish to contact our DPO please email contact@bulletproof.co.uk

You also have the right to lodge a complaint with the Information Commissioner Office (www.ico.org.uk) if you think that we have denied or infringed any of your rights. You can contact them any of the following ways:
Via their website https://ico.org.uk/make-a-complaint/; or
call their helpline on 0303 123 1113; or
contact them via live chat service ico.org.uk/livechat

Changes To Our Privacy Notice

We will keep our Privacy Notice under review and will notify you of any updates by placing them in this document.

Approval Details

APPROVAL AUTHORITY:	**NEAL HARRISON**
APPROVAL DATE:	10/06/2024
VERSION NO:	9