# General Data Protection Regulations & Privacy Policy

We are GB Electronics Ltd, Converge Technology Ltd and GBE Converge B.V t/as GBE Converge

GB Electronics Ltd is a company registered in England and Wales under registration number 02674826.

Converge Technology Ltd is a company registered in England & Wales under registration number 08225307.

GBE Converge B.V is a company registered in Netherlands under registration number 28079665

Our registered office is at GBEC House, 31 Barnett Way, Barnwood, Gloucester, GL4 3RT. Our trading office is at GBEC House, 31 Barnett Way, Barnwood, Gloucester, GL4 3RT.

Our Data Protection Officers is Katherin Woods. Please contact us if you have any questions about how we use personal data on Katherine.woods@mitie.com.

We review our policy at least annually or sooner if regulations change or if we change our data handling processes. If no changes are apparent, then a new revision to this policy may not be required. This notice explains how we use and secure your personal information when using our website or when we are processing screening checks for you.

**Employees:**
**Why do we collect Personal Information?**
We collect personal data for the purpose of carrying out background screening checks under the requirements of BS7858 as outlined by our Regulators, National Security Inspectorate (NSI). Processing of data will be to fulfil our regulatory obligations and processing of data received from employees will be as a result of the consent we have obtained from them as part of the employee application to work for GBE Converge.

It is an operational requirement in order for us to be able to ensure that we as a company can pay you on time and ensure that we can provide for any medical emergency you may encounter whilst in our employ.

There may be additional information we are required to collect and retain throughout the period of your employment and this shall be discussed with you at the time of requirement.

We shall look to obtain company vehicle tracking movements (this does not include private vehicles) in order to best provide our clients with exact travel times to and from our client site locations which shall be imported to the CRM software. We may use this information to ascertain best routes, driver safety and reduce fuel consumption, it will also provide benefits to our insurance premiums.
There will be no individuals information stored within the tracking unit as it shall be assigned to the company vehicle, however, given that some employees are issued a company vehicle which will return to the employees home address this information will understandably be tracked whilst the vehicle is on. Any information gained whilst the employee is not in work (weekends and annual leave) shall be disregarded and deleted throughout the course of the annum

**What Personal Information do we collect?**
The following is a list of personal details that we collect in order to process your employment application, some of which shall be passed on to our approved third-party suppliers (listed below):

- Name (inc any previous names)
- Date of Birth
- Place of Birth
- Sex
- Nationality
- Address (inc Previous addresses for up to last 5yrs)
- Identification (can include drivers license, passport, birth certificate)
- National Insurance Number
- Contact details (mobile number, landline, email)
- Employer & Character References
- Next of Kin contact details (Name, Address, Telephone No)
- Curriculum Vitae
- Relevant Employment information (Job Description, Contract & T&Cs of employment, Holiday Records, Sickness Records, Appraisal Forms, Occupational Health Records, Risk Assessment (pregnant & breastfeeding and/or Young Workers), Vehicle Tracking information (if applicable)

**Who will we share your Personal Information with and why?**
We will only share your personal data with a third party if we have your consent to do so, if it is necessary to fulfil contractual obligations to you, or if we are obliged to do so by law (e.g. Police investigation). If we have your consent to share your personal information for a certain requirement, this does not mean we will share your personal information for all elements of processing. We will obtain consent for each requirement as required.

**Personnel File Contents**
We shall hold in addition to the above information within your electronic personnel file located on the company server and job role specific, this information may also be saved within relevant SharePoint folders. Further details are detailed in Personnel Files Policy GBECPF100

**Sub-Contractors & Suppliers:**
In order to become an approved sub-contractor for GBE Converge you will be required to complete and return the Approved Supplier Questionnaire (PRO006-1) along with any supporting documentation as required within the form which includes but not limited to:

- copies of insurances
- training certification
- bank details
- contact information
- and compliance to the current Health & Safety Rules & Conditions for Sub-Contractors (PRO006-4)

Upon acceptance, any issued purchase orders shall also be accompanied by either Subcontract Labour T&Cs (PRO006-2), Purchase T&Cs (PRO006-3), Subcontractors Template (Installation) PRO006-8 or Subcontractor Contract Template (Commissioning) PRO006-12 or multiples thereof depending on the type of works to be undertaken on behalf of GBE Converge.

Whilst under the company's employ, you shall also be subject to any associated requests of PII as per our employees to ensure that the company remains compliant with its external governing bodies, which may include being credit checked and undergoing security screening to BS7858 depending on the works you are to undertake on behalf of the company.

Where the company legitimately feels it needs to check the honesty of its sub-contractors, they shall request from third parties (usually a client) to confirm the accuracy of any time sheets and/or overtime requests to verify any additional associated costs against issued Purchase Orders. This may be through the form of sign in/ out sheets, barriers, turnstiles which may involve biometric or photographic information.

Where you have provided to us services in order to complete a contract(s) and your working ethic or quality of services provided is of a poor standard, following internal review by the Operations Team & Contracts Director your details may be deleted from our system prior to the expected term of 6years. Should you wish to re-engage with us you will be required to complete an Approved Contractor Questionnaire PRO006-1 and shall be assessed on an ongoing basis to ensure same failings do not reoccur.

By becoming an approved subcontractor and/or supplier you agree to this process at any point during your employment with GBE Converge.

**Clients:**
**Why do we collect Personal Information?**
We collect personal data for the purpose of contractual obligations in order to provide the services that we offer as a business to include the Design, Supply, Installation, Commissioning & Maintenance of Fire & Life Safety Systems, Security Systems, Fixed Gaseous Suppression Systems and Network & Technology Systems.

*From Visitors to our website:*
When someone visits www.gbeconverge.com we use a third-party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website. If we do want to collect personally identifiable information through our website, we will be up front about this. We will make it clear when we collect personal information and will explain what we intend to do with it.

If you use our contact form, we will collect your name, email address and if you provide it within the message text area, telephone and/or address details so we can respond to your request for information.

*From callers:*
If you ring us we will collect your name, contact number and email address so we can respond to your enquiry.
If you are calling in relation to an active service agreement to place a fault call, then additional information may be requested to confirm the site location, the fault in question, IP address, Asset ID to allow remote connection, a site contact name and telephone number if you are not present at the fault location. Additional specific information may be collected to suit the specific needs of the caller.

**What Personal Information do we collect?**
The following is a list of personal details that we could collect in order to process your enquiry or deal with your specific request of us:

- Company information - Name, address and contact details; legal ownership and registration details; trading address;
- Contact information - Contact name, job title, business address, business phone number/ mobile number/ email address.
- User information - Contact name, job title, business phone number/ mobile number/ email address. Passwords for system software may also be collected in line with

providing remote support to users. The user shall be asked to change their password on next login to retain security of the account, although this may be changed prior to next login by the user.

- Site information – asset details to include type, location, make, model. As-fitted drawings of the building/ floor footprint with associated assets and identification numbering in place. Configuration files of system set up to include device type, make, model and location.

In the course of providing technical support to you, we may sometimes have incidental access to data that is located on your system, which may include special category data (primarily health). This data may contain information about you, your organisation's employees, clients/customers, patient data, partners, or suppliers. This Policy does not apply to our access to or handling of this information; the conditions regarding the handling and processing of that data is covered by the terms and conditions between you and us.

Unless you request us not to do so, we may also contact those employees of the customer who are involved in the delivery of the contract on an individual basis about similar services which we offer, this contact may be made by telephone, e-mail or post. We will never contact our client patients as these are persons not directly involved with our customer contract.
We will only do this if we believe that you would reasonably expect us to contact you in this way. We will not send you general marketing information as part of a group mailing, e-mailing or telephone campaign unless you have consented to be contacted in this way.
If you require your contact information to be removed from our system, Destruction of Documentation is detailed within *QAP001 Control of Documented Information* which is available on request, compliance@gbeconverge.com

**We have Received your Information from a Third Party**
If we have received your personal information from a third party, for example your employer or service provider, that third party will be the controller in relation to that personal information and we will be processing it on their behalf. You should therefore contact that third party to review their privacy policy.
Your Relationship with us is not Covered by any of the Above

We may hold your contact details and personal information as a result of an interaction between you and one of our employees. We believe that you would reasonably expect us to process your personal information in this way and that such processing does not an impact on you in a way that would make this processing unfair. We carry out a review of our contacts database every 2 years when we consider whether or not we still have a legitimate interest to keep your contact information.

**Below are the data processors we use during the screening process:**

*Police National Computer (PNC) Checks*
Police National Computer Checks (PNC) are processed by Gloucestershire Constabulary and they will hold the information that you submit as part of your employment application.
Here is a link to their Privacy Notice:

*National Security Screening Agency (NSSA)*
Security Screening Checks are processed by NSSA and they will hold the information that we collect until your screening application has passed (normally 12weeks up to a maximum of 16weeks). At the point of successful screening, all information held about you is destroyed by them.
Here is a link to their Privacy Notice: http://www.7858.co.uk/privacy-notice/

*Disclosure and Barring Service*
Criminal Record Disclosure applications are processed by the Disclosure and Barring Service and they will hold the information you submit and we will have access to it.
Here is a link to their Privacy Notice:
https://www.gov.uk/government/organisations/disclosure-and-barring-service/about/personal-information-charter

**Below are the data processors we use as part of any credit checking facilities**

*Experian*
Experian assesses information over a period of 6 years which can be found via public information, such as electoral roll and court judgments and from credit history information, such as existing lending agreements such as mortgages & car hire agreements.
Here is a link to their Privacy Notice:
https://www.experian.co.uk/legal/privacy-statement.html?_ga=2.266712077.201027559.1542986249-1728220090.1542986249

We may provide personal information to our approved suppliers & contractors in the event of ordering of equipment as part of spares & repairs or installation works. This information will include a Site Contact Name and Number and Site Address. All of our suppliers and contractors have been approved via our Procurement Team and our PRO006 Procurement Procedures as part of ISO9001.

**Our Regulators**

*National Security Inspectorate*
We are regulated by the National Security Inspectorate and during audit inspections they are given access to our screening files to ensure that we are carrying out screening in accordance with BS7858, ISO 9001 and all supporting British Standards.
Here is a link to their Privacy Notice: https://www.nsi.org.uk/privacy-statement/

*BAFE (British Approvals for Fire Equipment)*
We are regulated by BAFE via National Security Inspectorate and during audit inspections they are given access to our Project Site files to ensure that we are installing and maintaining in accordance with SP203-1 & SP203-3
Here is a link to their Privacy Notice: https://www.bafe.org.uk/privacy-policy

*Loss Prevention Certification Board (LPCB)*
We are regulated by the Loss Prevention Certification Board, they are given access to our Project Site files to ensure that we are installing and maintaining in accordance with LPS1014, LPS1204 & ISO9001 and all supporting British Standards
Here is a link to their Privacy Notice: https://bregroup.com/privacy-policy/

*SafeContractor (Alcumus)*
We are regulated by Safecontractor (Alcumus) for our SSIP Health & Safety certification. We upload supporting documentation onto their platform from which they can assess ouor Health & Safety record to confirm compliance to their certification. They may attend our premises to carry out site audits to satisfy the requirements of the scheme. This approval notice is then provided to CHAS, SMAS & Constructionline as part of a 'Deem to Satisfy' within the SSIP group of providers.
Here is a link to their Privacy Notice: https://www.alcumusgroup.com/privacy-policy

**Marketing and the use of your Personal Information**
We will only market services and products to you if we have your consent and at any time you can contact us and withdraw that consent and we will update our records accordingly.

**Accuracy of your Personal Information**
We work hard to make sure the data we hold is accurate, if you believe that the data we hold may be inaccurate then please contact us and we will correct any inaccuracies.

**Your rights**
Under the General Data Protection Regulations 2016, you have rights as an individual which you can exercise in relation to the information we hold about you.
You can read more about these rights here – https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

**Children's Privacy**
Our Services are not directed to children under 13. If you learn that a child under 13 has provided us with personal information without consent, please contact us.

**Complaints or queries**
We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.
This privacy policy was drafted with brevity and clarity in mind. It does not provide exhaustive detail of all aspects of our collection and use of personal information. However, we are happy to provide any additional information or explanation needed. Any requests for this should be sent to the address below.
If you want to make a complaint about the way we have processed your personal information, you can contact the ICO, the statutory body which oversees data protection law: www.ico.org.uk/concerns

**Access to Personal Information**
We try to be as open as we can be in terms of giving people access to their personal information. Individuals can find out if we hold any personal information by making a 'subject access request' under the General Data Protection Regulations 2016. If we do hold information about you, we will:
give you a description of it; tell you why we are holding it; tell you who it could be disclosed to; and let you have a copy of the information in an intelligible form.
To make a request for any personal information call us on 08451 220 884, email hr@gbeconverge.com or write to us: GBE Converge, Barnett Way, Barnwood, Gloucester, GL4 3RT. If you agree, we will try to deal with your request informally, for example by providing you with the specific information you need over the telephone.

**Security of your Personal Information**
Security of the information we hold is paramount.
All information is stored either at our Head Office in Gloucester or hosted within Office 365 in the EU. A back up copy is available either at our Data Centre in Gloucestershire or Data Centre in Slough.
Access to data within our server system is restricted dependent on job role and description. Individuals desktops or laptops have been encrypted to ensure that security to each machine or portable device is unlikely to be compromised.
Supporting policies including IT Resource and Use & Password Policy ensures that our employees do not abuse the equipment with which they are issued to complete their job roles successfully nor attribute to the incorrect disposure of client specific personal information.

All databases are hosted on Microsoft Azure within the UK which are ISO27001, ISO 9001 and ISO 20000-1 certified and also has CSA STAR Certification. Information on these certifications can be found at https://www.microsoft.com/en-us/trustcenter. Access to the database is restricted by IP address and requires unique username and strong passwords. All databases employ Microsoft's encryption of data at rest and on critical data such as Personal Data we have deployed further encryption measures to protect the Confidentiality. Our UK data centres are ISO27001, ISO 9001 certified and information on this can be found at https://www.iomart.com/about-iomart/accreditations/. Enterprise level Unified Threat Management systems are deployed to control access to all applications and locations. Access to all data is limited based on a strict access control policy. Access and operational logs are retained and audited on a regular basis. Any systems that process credit card data are PCI-DSS Certified and subject to strict auditing procedures. In addition to the above we have services that are Cyber Essentials accredited. This means our systems have been independently assessed and approved with regard to their ability to protect against common cyber-attacks.

**Links to other websites**
This privacy policy does not cover all the links within our company site linking to other websites. We encourage you to read the privacy statements on the other websites you visit.

**Cookies Policy**
To make the company site (www.gbeconverge.com) work correctly, we sometimes place small data files called cookies on your device. This is considered a standard procedure and most big websites do this too.

**What are cookies?**
A cookie is a small text file that a website saves on your computer or mobile device when you visit the site. It enables the website to remember your actions and preferences (such as login, language, font size and other display preferences) over a period of time, so you don't have to keep re-entering them whenever you come back to the site or browse from one page to another.

**How do we use cookies?**
Google Analytics, which uses cookies to help us analyse how our visitors use the site. Find out more about how these cookies are used on the Google Privacy site (https://support.google.com/analytics/answer/6004245)

**Data Breach Process**
Any breach of Personally Identifiable Information (PII) must be reported to the Data Protection Officers (DPO) within 24hrs of becoming aware of the breach. This is to allow sufficient time to investigate the cause of the breach, the date of the breach (if different from the awareness date), the method of the breach (softcopy or hardcopy) and to assess the risk and potential damage that the breach may cause to the individual(s) and/or the company.

Data Breaches must be reported to the ICO within 72hrs of awareness to the breach, preferably with confirmation of the resolution and measures to avoid further breaches.

If a hardcopy breach, such as loss of a notebook or As-Fitted Drawings, or softcopy breach, such as emailing PII to an incorrect recipient or a user's machine is hacked or compromised from an external source, the DPO's shall conduct internal interviews with those employees and/or subcontractors directly involved with the breach to ascertain the situation regarding why there was a need for PII to be on their person, location of the breach such as office, site or public transport and if required, instigate refresher training and/or disciplinary action as required.

In the event that a breach has occurred due to an employee or subcontractor having sold PII for financial gain, this shall be classed as gross misconduct as per the Company disciplinary procedure, the subcontractor shall be removed from the Approved Contractor listing and the breach may also be reported to the local authority.

The DPO's shall contact the individual(s) to which the PII relates to advise them of the breach, the extent of the information that has been breached and to clarify the individuals own risk and potential damage unto themselves. The individual(s) shall be invited to asses the findings of the breach reported by the DPO's.

**How We Secure Personal Information**
The Company takes data security seriously, and we use appropriate technologies and procedures to protect personal information. Our information security policies and procedures are closely aligned with widely accepted international standards and are reviewed regularly and updated as necessary to meet our business needs, changes in technology, and regulatory requirements.

| | |
|---|---|
| **Two factor authentication (2FA)** | Used where possible on business systems both on Premise and Online |
| **Password Controls** | Passwords for systems are controlled and stored centrally with security access to only permitted staff |
| **Employee vetting** | All staff are security screened to BS7858 that may have to handle/ review or process information. |
| **Physical Security** | Access to ours offices is secured with electronic access control and CCTV monitoring in place |
| **Encryption** | We use disk encryption for portal data and industry standard encryption technology for data encryption for data in transit and backups |
| **Training** | Our staff are appropriately trained for the awareness of data protection and security |

**Request for Information**
Individuals may make a Request for Information via various means of communication such as social media, verbally or via email to any employee of the company. Employees should pass on any such request to the Data Protection Officers or compliance@gbeconverge.com as soon as is practically possible.

The Request for Information should be logged against *QAP001-13 GDPR Acceptance & Destruction Record.*

The company has 1 month in which to respond to the request (or by the last working day of the following month from receipt of the request) and shall only provide information pertaining to the individual and not divulge any other information that is not directly related to said individual, unless they are working on behalf of the individual such as a solicitor i.e. the individual forms part of an FM company that manages a third party client site. The client site would need to provide consent to the company that the Request for Information was genuine and permitted.

The company may ask for proof of identity of the individual, the month in which to provide the requested information shall begin upon receipt of acceptable Identification.

The company shall confirm to the individual that:
- We are processing their personal data

- Provide a copy of their personal data
- Provide other supplementary information including;
    - Retention period(s)
    - Right to lodge a complaint with the ICO
    - Source of the data (if not obtained directly from the individual)
    - Existence of automatic decision making (inc profiling) if applicable

If the PII we hold is in a handwritten format, this information shall be provided. We are not required to make hand written notes legible. The information that we provide shall be in English. No other languages shall be provided, you should seek to have the information translated to suit your own needs.

If the information held about the individual also relates to another individual, we may withhold issuing such information against Data Protection Act 2018 unless the other individual has consented to its release

Where a Request for Information is manifestly unfounded or excessive then we reserve the right to charge a fee of £10 per request to cover any administrative costs incurred to or by the company.

**Destruction of Information**
After the retention periods detailed in *QAP001 Control of Documented Information* have lapsed, the archived information shall be securely disposed of by an approved third party contractor and shredded at no less than quarterly intervals.
A certificate of destruction shall be provided to the company to confirm the number of secure bags/ archive boxes that have been securely shredded. This certificate will not specifically detail the content of the secure bag/ archive box.

In line with General Data Protection Regulations (GDPR) and based on their being no reason as to why the personal information must be held for the required retention periods, personal information relating to a customer site or employee may be securely disposed of sooner upon receipt of a 'Request to Destroy Information'.

The following details shall be listed within the 'Request to Destroy Information' as applicable:
- First & Last Name of the contact
- Whether an employee, contractor or client
- Site or Project Name
- Detail of information to be destroyed (maintenance records, project records, personal information, marketing detail, other)

This shall be registered against *QAP001-13 GDPR Acceptance & Destruction Record* and the appropriate tab therein. The Company shall have a period of one month in which to destroy the information and advise the contact accordingly that their request has been processed.

Information is unable to be destroyed if the processing is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

The company may refuse to process a Request to Destroy Information if we consider that the request is manifestly unfounded or excessive and we shall contact the individual to clarify our reasons.

**Request to suppress processing of specific data**
An individual may request that their PII is restricted from processing. This only applies in certain circumstances:

- Where the individual contests the accuracy of their PII and the company is verifying the accuracy of the data held
- Where the data has been unlawfully processed and the individual requests restriction over erasure
- Where the company no longer requires the data but the individual asks the company to keep it in order to establish, exercise or defend a legal claim
- The individual has objected to the company processing their PII and the company is considering whether their legitimate grounds override those of the individual

Upon receipt of a Request to Suppress the company may either:

- Move the data to another processing system
- Make the data unavailable to users
- Or temporarily remove published data from a website or Social Media Page

Where the individuals PII has been disclosed to a third party company, the Company shall contact the third party immediately to advise them of the restriction to process.
If the Company, after assessment, decide that the restriction is unfounded over the Companies legitimate grounds of operation then the individual shall be contacted to advise that the restriction is to be lifted and the reasons why.

**Ensuring the Personal Data we hold is current**
The company from time to time may request updated information from either employees, clients or subcontractors. This request may be in the form of an email or letter.

The request could include (but may not be limited to) updates to contact names, numbers, email addresses, bank details, address details (inc registered offices and trading offices)

The request to clients and subcontractors could, in addition to the above, include confirmation of certification against accreditation bodies, health & safety statistics and any convictions or notices that may affect the working relationship between you and the company.

It is also the responsibility of the employee to proactively advise the company in any change in details or circumstances (inc medical requirements) that may affect how the company interacts with the employee.

Jason Buttle
Managing Director

Date: 24th December 2024