GPEC Group

Comprising:
G.P.E.C GROUP LIMITED (15267225)
G.P.E.C LIMITED (06612222)
G.P.E.C SUPPLY LIMITED (12325979)
G.P.E.C INTERNATIONAL LIMITED (15268959)

GPEC Group Policy 1.18 – Data Protection

Introduction

This Policy sets out how we handle the Personal Data of our customers, suppliers, employees, workers and other third parties. It is intended to incorporate our obligations under the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) ("UK GDPR") and the Data Protection Act 2018.
This Policy applies to all Company Personnel ("you", "your"), and sets out what we expect from you in order to help us comply with the law in this area.

What is "Personal Data"?

When we talk about Personal Data, we are referring to any information which identifies or relates to an individual, for example a name, address, date of birth or email address. It also includes sensitive personal data, for example racial or ethnic origin, religious beliefs, sexual orientation or physical or mental health conditions.

What is "Processing" Personal Data?

We will mention process or processing Personal data in this Standard. By that we mean any activity that involves the use of Personal Data. It will include obtaining, recording or holding the data and also covers transferring the data to third parties (for example insurance providers or IT companies).

Scope

Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we must take seriously at all times. If we are in breach of any of our obligations under the UK GDPR, we are exposed to serious financial penalties. Given the seriousness of this subject, please be aware that any breach of this Standard may result in disciplinary action.
Whilst all personnel are responsible for complying with this Standard, Managers will be responsible for ensuring the compliance of their teams.

The DPO is responsible for overseeing this Policy, and that post is held by: *The Operations Director* Please contact he Operations Director with any questions about the operation of this Policy or the UK GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the Operations Director if you have any concerns about whether we are complying with the Personal Data Protection Principles set out below.

Personal Data Protection Principles

We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).
- Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**Data Minimisation**).
- Accurate and where necessary kept up to date (**Accuracy**).
- Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**Storage Limitation**).
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).
- Not transferred to another country without appropriate safeguards being in place (**Transfer Limitation**).
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (**Data Subject's Rights and Requests**).
- We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

Lawfulness, Fairness, Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
You may only collect, process, and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process Personal Data fairly and without adversely affecting the Data Subject.
The UK GDPR allows Processing for specific purposes, some of which are set out below:

- the data subject has given us their consent.
  In order to obtain relevant consent, an individual must indicate agreement clearly either by a statement or positive action. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.
- the processing is necessary for the performance of a contract, for example to sell a customer a valve or provide the customer with consultancy services;
- to meet our legal or compliance obligations, for example with HMRC;
- to protect the Data Subject's vital interests, which must be a life-or-death situation;
- to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process Personal Data for legitimate interests are set out in relevant Privacy Notices issued.

Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. We therefore only request personal data required to ensure successful business operations.

Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
You may only process Personal Data when performing your job duties requires it. You cannot process Personal Data for any reason unrelated to your job duties.
You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes. If you are unsure as to the reason or purpose for collecting data please speak to your manager.
You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines.

Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.
You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.
If you have any concerns regarding the accuracy or updating our client records please contact your Line Manager. For employee records please contact the Operations Director.

Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.
You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.
You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Security, Integrity, and Confidentiality – Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
We will develop, implement and maintain safeguards, including cyber security measures and appropriate hardware security measures. You are responsible for protecting the Personal Data we hold and you must exercise particular care when collecting and processing any Personal Data to avoid loss and unauthorised access, use or disclosure.
You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer

Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.
You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

Reporting A Personal Data Breach

The UK GDPR requires us to notify any Personal Data breach to the applicable regulator and, in certain instances, the data subject.
If you know or suspect that a Personal Data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Operations Director. You should preserve all evidence relating to the potential breach.

Transfer Limitation

The UK GDPR restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.
You may only transfer Personal Data outside the UK if requested as part of your job role.

Data Subjects Rights and Requests

Data subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw consent to processing at any time;
- receive certain information about our processing activities;
- Request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the UK;
- prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- be notified of a Personal Data breach which is likely to result in high risk to their rights and freedoms; and
- make a complaint to the supervisory authority.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).
You must immediately forward any data subject request you receive to the Operations Director.

Accountability

We have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

- appointing a suitably qualified DPO/MANAGER accountable for data privacy;
- implementing appropriate measures when processing Personal Data and completing Impact Assessments where processing presents a high risk to rights and freedoms of data subjects;
- integrating data protection into internal documents including this Policy, related policies and our Privacy Notices;
- regularly training Company Personnel on the UK GDPR and this Policy;
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

Record Keeping

The UK GDPR requires us to keep full and accurate records of all our data processing activities.
You must keep and maintain accurate records of any Personal Data you collect or process during your duties.

Training and Audit

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.
You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.
You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.
When carrying out your duties, please assess what Privacy by Design measures can be implemented or improved on any programs/systems/processes that you use.
We will also conduct DPIAs in respect to high-risk processing.

Automated Processing (Including Profiling) and Automated Decision Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual.
If a decision is to be based solely on Automated Processing (including profiling), then data subjects will be informed when we first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information.
Further, suitable measures must be put in place to safeguard the data subject's rights and freedoms and legitimate interests.
We must also inform the data subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the data subject the right to request human intervention, express their point of view or challenge the decision.
A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.
You may only share the Personal Data we hold with another employee, agent or representative of our group the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.
You may only share the Personal Data we hold with third parties, such as our service providers (pension providers, insurance companies etc) if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with our Privacy Notice;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains UK GDPR approved third party clauses has been obtained where necessary.

Changes To This Policy

We reserve the right to change this Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Policy.
This Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

Declaration of Compliance

THE FOLLOWING CERTIFICATION WILL BE SIGNED AT REGULAR PERIODS DETAILED BELOW TO CONFIRM COMPLIANCE WITH ALL APPLICABLE LAWS IN ALL RELEVANT JURISDICTIONS

To be completed by a Company Director

Name: Scott Gower

Entity name: GPEC Group

Renewal Date:

Please report any changes or relevant information relating to this policy here:

I confirm that the information I have provided above remains true and accurate to the best of my knowledge. I confirm that if I should learn of any information regarding any such violation, I will immediately advise public officials where necessary.

Name: Scott Gower

Title: Company Director

Dated:

Signed: