

Introduction

As a business, Press Commercial Bodyworks Ltd, needs to keep and process personal information relating to our employees, customers, suppliers and other parties in order that we can provide services for accident repair, repainting, re-livery, and body repairs, to manage our business relationships effectively, for the administration and promotion of our business.

The EU General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA) (which supersedes the Data Protection Act 1998 in May 2018) governs how we process personal information within the UK.

This Policy sets out how we will comply with that Data Protection legislation, explaining how we will seek to protect personal data and ensure that our employees understand the rules governing the use of personal data to which they have access in the course of their work.

We are committed to ensuring that all personal and sensitive data that we hold about individuals is accurate, up to date, only used for the purposes intended and securely protected by us.

Definitions

Business purposes

The purposes for which personal data may be used by Press Commercial Bodyworks Ltd:

Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- This Policy supports our Information Security employee guidance
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking (where used and is appropriate)
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing employee access to systems and facilities and employee absences, administration and assessments
- Monitoring employee conduct, disciplinary matters
- Marketing our business
- Improving services

Personal data 'Personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified, such as name, identification number, location data or online identifier (IP address). This applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria.

Examples of personal information relating to identifiable individuals that would apply to Press Commercial Bodyworks Ltd, include job applicants, current and former employees, agency, contract and other employees, customers, suppliers/contractors, site visitors, and other industry contacts.

Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, pensions, health, marital status, nationality, job title, and CV.

Sensitive/ special categories of personal data Personal data about an individual's race; ethnic origin; politics; religion; trade union membership (or non-membership); genetics; biometrics (where used for ID purposes); health (physical or mental health or condition); sex life; or sexual orientation.

Any use of sensitive/special category personal data will be strictly controlled in accordance with this Policy.

Please note that in order to manage the employment contract and to comply with Health & Safety requirements, other legislation, and in order to pursue our own legitimate interests, Press Commercial Bodyworks Ltd would only typically process health data. It is very unlikely that we would request and process other special category data listed above.

Data Controller A controller determines the purposes and means of processing personal data

Summary of data protection principles To ensure that personal data is only:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Scope

This Policy applies to all Press Commercial Bodyworks Ltd employees. All employees that process personal data must be familiar with this Policy and comply with its terms.

This Policy supports our Information Security employee guidance. We may supplement or amend this Policy by additional policies and guidelines from time to time. Any new or modified Policy will be circulated to employees before being adopted.

Responsibilities

Press Commercial Bodyworks Ltd is the Data Controller for the purposes of processing personal data under the current Data Protection legislation. We are registered with the Information Commissioner's Office (ICO) under registration no. ZA329757.

Emma Warren (Company Director) is responsible for data protection at Press Commercial Bodyworks Ltd and has overall responsibility for the day-to-day implementation of this Policy to ensure that we comply with the Data Protection legislation. A summary of those responsibilities are as follows:

- Keeping the Board, senior managers and key employees updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all employee members
- Answering questions on data protection from employees, the Board, senior managers and other stakeholders

- Responding to individuals such as customers and employees who wish to know which data is being held on them by Press Commercial Bodyworks Ltd
- Checking and approving with third parties that handle the company's data, any contracts or agreements regarding data processing
- Ensure all IT systems, services, software and equipment meet acceptable security standards (via the company's IT support provider)
- Checking and scanning security hardware and software regularly to ensure it is functioning properly (via the company's IT support provider)
- Researching third-party services, such as cloud services the company is considering using to store or process data (via the company's IT support provider)
- Ensure all marketing initiatives adhere to data protection laws and this Data Protection Policy
- Approving data protection statements attached to emails and other marketing communications/activities
- Addressing data protection queries

All employees that come into contact with other people's personal data are responsible for ensuring it is handled in relation to this Policy and to ensure that information security standards are maintained.

How we comply

The following sets out how Press Commercial Bodyworks Ltd will comply with the Data Protection legislation and we will ensure that any processing is in line with the data protection principles.

Fair and lawful processing

We will process personal data fairly and lawfully in accordance with an individual's rights. This generally means that we should not process personal data unless either the individual whose details we are processing has consented to this happening or we are required to process the personal data for another lawful reason.

We will ensure that the processing of all personal data must be:

- necessary to deliver our services
- only conducted if a suitable lawful reason can be identified, as set out within the Data Protection legislation (called 'conditions for processing'). The following examples will typically apply to us:
 - to comply with law;
 - to fulfil or in preparation of a contract;
 - for our own legitimate interests;

- in an emergency situation to protect the vital interests of the individual or another person; or
 - we have obtained the consent of the individual.
- in cases of processing sensitive/special category personal data, we will only process if we can meet a further lawful reason to permit that processing (called 'conditions for processing special category data'). The following examples will typically apply to us:
 - we need to exercise our rights or that of the individual within the field of employment;
 - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee;
 - processing is necessary for the establishment, exercise or defence of legal claims;
 - processing is necessary to protect the vital interests of the individual or of another natural person where the data subject is physically or legally incapable of giving consent; or
 - obtaining the explicit consent of the individual

We recognise that sensitive/special category data could create more significant risks to a person's fundamental rights and freedoms, such as by putting them at risk of unlawful discrimination and therefore extra care will be afforded in order to protect the integrity of that data.

- within our legitimate interests and to not unduly prejudice the individual's privacy
- done in such a way to preserve an individual's information rights
- transparent and to provide accessible information to individuals about how we will use their personal data, in the form of a Privacy Notice as explained below.

We will only disclose information about an individual to third parties if we are legally obliged to do so (such as Law Enforcement agencies) or if we have a genuine legitimate business interest that does not undermine the individual's own rights and interests, and it is done in a way that is reasonably expected.

Privacy Notice

How we use personal data within our business activities is explained within our Privacy Notices, which are available on our website <http://www.presscommercials.co.uk/privacy.html>

The notice sets out:

- the purposes for which we hold and process personal data for individuals, such as our employees, customers and suppliers
- highlights that our work may require us to give information to third parties
- that individuals have information rights, such as the right of access to the personal data that we hold about them, and how they can go about exercising those rights.

We make our Privacy Notices available in various mediums, such as on our website, website links attached to various external facing documents, such as on our invoices, purchase orders, quotes, emails, printed copies available at our site and can provide copies on request.

Consent

Where processing is enabled with the consent of the individual, we will clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. Consent requires a positive opt-in and we will not use pre-ticked boxes or any other method of default consent.

Consent will be recorded by us and the individual will be advised that they have the opportunity to withdraw consent, how they can do this and if there are any implications to that process.

If 'explicit consent' is required for the processing of sensitive or special category personal data, we will ensure that we obtain their written consent, the reasons why we need consent for processing and the individual's rights associated with that consent are provided to them.

Please note that consent is not required if we are processing personal data under other lawful conditions, such as by law.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If an individual believes that information is inaccurate, they should record the fact that the accuracy of the information is disputed and inform Emma Warren – Company Director (details at the end of this Policy).

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons why that the personal data was obtained, but should be determined in a manner consistent with our Data Retention Schedule, which is in accordance with other legislation, industry guidelines and best practice.

HR records are reviewed annually to ensure that they comply with our Schedule and any information that has reached its retention period or if no longer required for the purpose, is either shredded or securely deleted.

The Data Retention Schedule is also reviewed on an annual basis.

Employee data

All employees must take reasonable steps to ensure that personal data we hold about them is accurate and updated as required. For example, if personal circumstances change, please inform Emma Warren so that these can be updated immediately. As a matter of routine, we will contact all of our employees on an annual basis to ensure that their contact details are up to date, and provide them with a copy of the current Employee Privacy Notice.

An Individual's information rights

Under the Data Protection legislation an individual has the following rights with regards to their personal data that we collect, hold and process:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Right to be informed

The right to be informed that processing is taking place is set out within our Privacy Notice. In addition with information on the right to be informed, who is collecting their data, purposes for processes, who it will be shared with, how they can exercise their rights and if they have a query or complaint, who to contact.

The right of access

Individuals are entitled, subject to certain exceptions, to request access to information that we may hold about them, which is called a Subject Access Request (SAR). This will help the individual understand what information we hold and if any of the information is inaccurate, which will provide them with the opportunity to get it rectified or updated. We will respond to such requests in writing within the statutory one calendar month. We will ensure that any information that we are lawfully required to provide does not compromise the privacy of other individuals.

We do not charge for processing SARs, however, in the event that the request is manifestly unfounded or excessive, we are allowed to charge a "reasonable fee" for the administrative costs of complying with the request and for providing further copies of data following a request.

All of our office employees are trained in how to recognise a SAR and all such requests are managed and processed by Emma Warren.

In the event that an individual would like to submit a SAR request, please put the request in writing to Emma Warren (address at end of the Policy) including the following points, which will help us to identify the necessary information:

- Name and Contact details
- Form of ID (such as a driving licence/passport so we can verify for identity)
- In what capacity we may hold your information, such as a site visitor, customer, supplier, employees etc.
- Any relevant date ranges or events that you are interested in
- How you would like to receive the information (format)

Please note that for a third party acting on behalf of the individual, any requests should be on official headed paper and accompanied with a letter of written authorisation from the individual and a copy of the individual's ID to confirm their signature.

Further information about SARs is available on the ICO website: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/>

Rights to rectification, object, data erasure and restrict processing

Along with the right of access, an individual has the right to request rectification of their personal data if incorrect. In certain circumstances, an individual may have the right to restrict processing, object to processing, and data erasure if we have no lawful or genuine reason to continue to hold it. Any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

We currently do not undertake automated decision making and profiling for personal data, but in the event that we do, we will advise the individual of their data rights. Data Portability allows an individual to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. This is mainly aimed at services such the utility and the banking industry. However, we will always work with the individual to provide the information that they require in a suitable format.

Please note that we will actively uphold an individual's information rights unless they are subject to certain exemptions under the Data Protection Act 2018, such as for the prevention and detection of crime.

Data Security

In order to maintain the security and integrity of our personal data, we have in place the following:

- Employees who come into contact with personal data as part of their job will be issued with guidance and training about how they can store and process that data securely
- There are secure areas on site where personal data is stored
- We will ensure that our employees have the correct resources to keep the information safe, such as IT security features, shredders, locked draws, and encrypted memory sticks (should there be a valid reason for taking data outside of the office/and or disclosing it to legitimate third parties)
- We will maintain physical security for our site, such as CCTV and secure office space
- IT data will be regularly backed up in line with the company's backup procedures
- All IT servers containing sensitive data will be approved and protected by security software and strong firewall
- Where other organisations that process personal data as a service on our behalf (data processors), we will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations

Please note that all employees are responsible for keeping **their own personal data in their possession** secure against loss or mis-use. Should an employee require assistance in how they can keep their own information safe, please contact Emma Warren.

Employee Training

Employees who are responsible or come into contact with personal data will receive training on this Policy and for information security awareness. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our Policy and procedures. Completion of training is compulsory.

A copy of this Policy will be available for all employees in order to raise general awareness in the workplace, regardless of whether they handle personal data or not as part of their role.

Criminal Offence data

In the event that we are required to process data about criminal convictions, criminal offences or related security measures, we will ensure that we meet the lawful processing conditions for this as set out within the legislation, for one that meets the lawful basis for processing, and a criminal offence data condition. Both of these will be documented to ensure we can demonstrate compliance and accountability. Any criminal record checks that we are required to undertake must be justified by law.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. Emma Warren will be responsible for conducting a Data Protection Impact Assessment (DPIA) and will ensure that all IT projects and any new projects that can impact on privacy such as new CCTV systems commence with a privacy plan and are duly risk assessed.

When relevant, and when it does not have a negative impact on the individual, privacy settings will be set to the most private by default.

International data transfers

The processing of any personal data by us currently takes place within the European Economic Area (EEA). However, in order to comply with our legal and contractual requirements, it may be necessary to transfer personal information to an international organisation outside of the EEA. If such circumstances arise, we will ensure that the appropriate controls are put in place to protect that data. Our Privacy Notices will be duly updated to inform the individual if their personal data is being transferred outside of the EEA.

Contracts

- We will only appoint Data Processors (who process our personal data on our behalf) who can provide 'sufficient guarantees' that the requirements of the Data Protection legislation will be met and the rights of data subjects protected.
- We will review on a regular basis all of our existing Data Processor contracts to ensure that they meet our needs and that of the Data Protection legislation.

- We will ensure that we carry out the necessary due diligence so that they meet our needs for processing and information security.
- Whenever we use a Data Processor for the processing of our personal data on our behalf, we will ensure that there is a written contract in place.
- If a contractor requires access to our personal data (such as for IT maintenance reasons), we will ensure that there is either a written contract or a Confidentiality Agreement in place.
- The contract or Agreement will ensure that that all parties understand their responsibilities and liabilities.
- Data Processors must only act on our documented instructions (such as those set out in a Schedule of Processing), however, processors now have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply with the legislation.
- Organisations that provide professional advice, such as accountants and solicitors are Data Controllers in their own right, however, we will ensure that there is a suitable contract in place to advise on the terms of business and so that all parties are aware of their responsibilities and liabilities.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All employees have an obligation to report actual or potential data protection compliance failures or data breaches. This allows us to:

- investigate the failure and take remedial steps if necessary;
- maintain a register of compliance failures; and
- in cases of high risk data breaches, to notify the Information Commissioner's Office (ICO) of any compliance failures that are material either in their own right or as part of a pattern of failures within 72 hours of the breach being detected.

Monitoring

All employees must observe this Policy. Emma Warren has overall responsibility for this Policy and will monitor it regularly to make sure it is being adhered to.

The Policy will be reviewed annually or if a change is required due to an update in the legislation or an internal process.

Consequences of failing to comply

We take compliance with this Policy very seriously. Failure to comply puts individual employees, the organisation and for those whom we process their personal data at risk.

The importance of this Policy means that any employee who fails to comply with any requirement may lead to disciplinary action.

Further Information and Complaints

For any questions about this Policy, please contact Emma Warren (Company Director), at **emmaw@presscommercials.co.uk**, telephone **01179 821166** or you can write to us at **Press Commercial Bodyworks Ltd, Units ABCD, Smoke Lane, Avonmouth, Bristol, BS11 0YA**.

If an individual is not satisfied about the way that we process personal data, they have the right to lodge a complaint to the Information Commissioners' Office (www.ico.org.uk) if they believe that we have not complied with the requirements of the General Data Protection Regulations (GDPR) or Data Protection Act 2018 (DPA), however, we would appreciate if you could contact us first to investigate your concerns.

The Information Commissioner's website is also a good source of information

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>