P + H BODY REPAIRS LTD

GDPR Data Protection Policy

Last updated 14/05/2018

This is a statement of the Data Protection Policy adopted by P + H BODY REPAIRS LTD.

Responsibility for updating and dissemination of this policy rests with P + H BODY REPAIRS LTD owner and senior management. The policy is subject to regular review to reflect changes in legislation. All staff are required to understand, apply and abide by the policy and if in any doubt to seek advice.

All staff, regardless of department, must receive General Data Protection Regulation and Data Protection Act 1998 awareness training as part of a signed induction process. Ignorance of the GDPR and DPA (98) is unacceptable.

P + H BODY REPAIRS LTD collects and uses certain types of personally identifiable information about clients, customers and suppliers in order to operate. This includes current, past and prospective individuals and entities with whom we conduct business. Personal information, or data, must be dealt with properly however it is collected, recorded and used – whether on paper, electronically, or other means.

The success of our operation and achievement of our objectives depends upon maintaining confidence of those we do business with. Therefore, we need to ensure we treat personal information lawfully and correctly. In doing so, we fully endorse and adhere to the GDPR and the principles set out in the DPA (98).

The eight principles of the DPA (98) are:

1. Data shall be processed fairly and lawfully and not processed unless specific conditions are met
2. Data shall be obtained for specified and lawful purpose/s, and not further processed in any other manner
3. Data shall be adequate, relevant and not excessive in relation to the purpose processed
4. Data shall be accurate and, where necessary, kept up to date
5. Data shall not be kept for longer than is necessary for the specified purpose
6. Data shall be processed in accordance with the rights of the data subjects under the Act
7. Data should be subject to technical and organisational measures to prevent damage, destruction or loss
8. Data shall not be transferred outside the EEA unless the country has an adequate level of data protection

(These will be replaced by the GDPR in May 2018)

In relation to the GDPR, there are 7 Principles and 8 Rights that have to be observed:

Principles	**Rights**
1. Legality, Transparency and Fairness	1. The right to be informed
2. Purpose Limitation	2. The right of access
3. Minimisation	3. The right to rectification
4. Accuracy	4. The right to erasure
5. Storage Limitation	5. The right to restrict processing
6. Integrity and Confidentiality	6. The right to data portability
7. Accountability	7. The right to object
	8. Rights in relation to automated decision making and profiling

(These come into force in May 2018)

We ensure that:

- We complete and regularly update a personal data risk register
- We attend and review a personal data training and awareness programme
- We appoint a senior manager with overall accountability and responsibility for personal data
- We review and update our data protection policy as new legislation emerges
- We understand what personal data we hold, where it's held and where it goes
- We have a legal basis for our data processing activities
- We understand and properly define our processing activities
- We have enforceable written personal data handling agreements with all third party suppliers
- We carry out appropriate due diligence on all third party suppliers
- We complete and regularly review our data privacy impact assessment

- We update and regularly test our incident management policy
- We attend to any subject access requests (SAR) in a timely manner (less than one month)
- We rectify, restrict and allow portability of data via safe means
- We review and update our information security policy on a regular basis
- We update our annual registration with the ICO
- We align ourselves, as much as possible, with the objectives and requirements of ISO 27001
- We meet the requirement of the Cyber Essentials accreditation
- We check that all the above is kept in order via an appropriate compliance programme

Version History

01 – Data Protection Policy 01022018 – initial document approved by MATTHEW POLLITT