	Data Protection Policy	BS(D).05.01 July 2019

1. Scope

This policy applies to all employees, current, past and prospective, together with those contracted to work at or for the company and may include members of the public, clients, customers, and suppliers.

Bridgestone will ensure that it treats personal information lawfully and correctly.

As both a data controller and a data processor, Bridgestone fully endorses and adheres to the principles of data protection as set out in the General Data Protection Regulations 2016.

2. Purpose

The purpose of this policy is to ensure that Bridgestone complies fully with its legal obligations in relation to the protection of personal data that it holds about or concerning any individual. All employees must familiarise themselves fully with its contents and ensure that its terms are applied fully in relation to the handling or "processing" of personal data.

Data protection laws are overseen by the Information Commissioner who has powers to take legal action against businesses or individuals acting unlawfully. This policy is designed to prevent such potential damage to the Company and its employees and to ensure that personal data processed by the company is dealt with in full compliance with the law.

3. Responsibilities

Whilst we do not require a DPO, we have ensured that appropriate mechanisms are in place for ensuring that data is protected, that data subjects are always informed about processes we may undertake with their data and that where required the appropriate consent is gained. Nominated persons will ensure that:

- The provision of data protection training, for employees.
- For the development of best practice guidelines.
- For carrying out compliance checks to ensure adherence, throughout the company, with the GDPR.

All staff are aware of their responsibilities, which include:

- Checking that any personal data that they provide to the company is accurate and up to date.
- Informing the company of any changes to information which they have provided, e.g. changes of address.
- Checking any information that the company may send out from time to time, giving details of information that is being kept and processed.
- Ensuring that any data they process is controlled in line with this policy and our internal processes to ensure that it does not affect any data subject's rights.
- Report any breaches within 24hrs to their manager.

4. Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes, and that it isn't processed in a different way than it was originally intended
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date;

e) 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;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing

In relation to point a), Bridgestone are required to determine a lawful basis for processing data.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others but we must choose the most appropriate. The lawful basis's are:

- Consent
- Legitimate interest
- Legal obligation
- Contractual obligation
- Vital interest
- Public task (only applicable to public bodies)

In relation to point b), we must ensure that the appropriate fair processing notice is in place, and this could be in the form of either a signed consent document or a privacy notice. These fair processing notices will contain the following information:

- Who holds the data
- Who it is shared with
- What the data is and what processes it is used for
- What is the determined lawful basis
- The retention period of said data
- The data subject's rights, and how to exercise them

All fair processing notices are controlled by the DPO and are recorded on a central register to track who they have been issued to and when. Where a new data process is required, the DPO shall be informed so that a new FPN can be drafted and issued prior to the process occurring.

In relation to points e) & f), Bridgestone operate a robust office protocol in relation to how data is managed, shared and retained.

Bridgestone also operate a central data register, recording the following:

- Document type, i.e. what document holds the data
- Subject Groups(s) and data field
- Storage Location(s)
- Access to data
- Department Owner
- Sharing details, both internal and external
- Retention periods
- PIR completed
- Lawful basis
- Consent or Privacy notice status
- Actions required
- Risks

This allows every person in the business to check that any process they wish to undertake has been assessed, what the retention periods are for each data field (to ensure they delete any data held by themselves in the adequate time period) and to confirm who data can be shared with and how it should be shared.

5. Privacy Impact Assessments

In some instances, where the risk to the individual's privacy is considered high, the information identified in the data register is subject to a Privacy Impact assessment.

6. Data subject rights

The GDPR provides the following rights for individuals:

- 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.

These rights are not applicable in every scenario and based largely in which lawful basis has been selected. For instance, where the lawful basis is a legal obligation, the data subject cannot object.

All requests to exercise these rights must be referred to the DPO to ensure they are responded to within the required time frame and actioned as legally required,

7. Sensitive/special category data

Special category data is more sensitive and therefore needs more protection because this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Sensitive personal data is defined as personal data consisting the following data types:

- Race;
- Ethnic origin;
- Political opinions;
- Religion;
- Trade union membership;
- Genetics;
- Biometrics (where used for id purposes);
- Health;
- Sex life; or Sexual orientation.

In these instances, as well as determining a lawful basis for processing, we also need to satisfy a specific condition under Article 9.

It should be noted that wherever possible Bridgestone endeavour to eliminate holding sensitive information to ensure the data subject is protected.

8. Data Security

Bridgestone will ensure that data is kept securely and that precautions will be taken against loss or damage, and that both access and disclosure must be restricted. Bridgestone are responsible for ensuring that:

- Any personal data which Bridgestone hold is kept securely;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Ensure that the rights of people about whom the information is held can be fully exercised under the regulation;
- Personal information is not disclosed to any unauthorised third party.

In addition, Bridgestone will ensure that:

- Specific responsibilities for data protection are assigned in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

9. Subject Access Requests

Any data subject has the right to request information on what data is being held and how it is being processed. All requests will be recorded and managed by the office manager with response being returned within 30 days.

10. Data Breaches

Under GDPR we have a responsibility to ensure that all breaches within the business are reported, no matter how minor.