



GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (GDPR) came into effect on May 25th, 2018, superseding the Data Protection Act 1998 and other Data protection Regulations. The primary purpose of GDPR is to protect the personal data of residents of countries within the European Union (EU).

The protection of people in regard to their personal data is a fundamental human right. The rules and guidelines within the General Data Protection Regulation are designed to support this premise. It states that all data controllers (organisations that collect and store user data) must protect the data, give users access to the data, and make the data easily transferrable.

GDPR updates the previous Data Protection Directive to be relevant to modern times and technologies. For example:

- Regulation 42 states that data processors (such as websites) must make their identity clear and ask users for consent before storing their data.
- Regulation 49 bans malicious activity in regards to data, such as hacking and denial of service attacks.
- Regulation 83 states that data controllers and processors should mitigate security risks by using encryption.
- Article 33.1 requires organisations to inform their users within 72 hours of when a data breach has been discovered.

The GDPR guidelines must be followed by all public and private companies and organisations within the EU. Fines and penalties may be assessed to entities that do not conform to the regulations. While GDPR is commonly associated with IT industries, such as e-commerce websites and cloud services, it applies to all EU organisations that store personal data.

While GDPR is enforceable within the European Union, it also applies to companies and organisations outside the EU that do business with EU residents. For example, if a U.S.-based company stores data for individuals living in Sweden, it must conform to the GDPR regulations. On the consumer side, GDPR protects both EU citizens and people who live and work in the EU. The rules apply to individuals engaged in business transactions, but they do not apply to personal or household activities.

GDPR compliance is important, as GDPR is a regulation that dictates specific requirements with which businesses must comply to protect the personal data privacy of EU citizens. The regulation also includes the monitoring of data that is exported outside the EU. Another aspect, which makes the GDPR so important, is the considerable amount of administrative fines non-compliance could subject companies to. Infringements of some provisions are subjected to fines of up to EUR 10,000,000 or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The British Woodworking Federation GDPR Policy is necessary, as it provides guidance to the organisation and outlines all the data protection responsibilities of its employees.



Definition of key GDPR terms:

➤ Controller

A data controller is a person, company, or other body that determines the purpose and means of personal data processing (this can be determined alone, or jointly with another person/company/body). If you are a controller, you are not relieved of your obligations where a processor is involved in a breach– the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

➤ Processor

A data processor is a person who processes data on behalf of a data controller. A data controller decides the purpose and manner to be followed to process the data, while data processors hold and process data, but do not have any responsibility or control over that data. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

➤ Data subject

Data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, date of birth, national insurance number etc. In other words, a data subject is an end user.

The GDPR's requirements apply to EU residents' personal data and anyone in the British Woodworking Federation who processes that information. The GDPR does not however apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

The British Woodworking Federation is committed to adhering to the seven main principles of GDPR. By ensuring that all personal data processed by its employees is done so, lawfully, fairly and transparently. That the personal data collected is limited to that data for which there is a specific purpose, minimising data collection. That the data collected and processed is done so accurately, limiting the amount of personal data stored. The British Woodworking Federation will ensure that any personal data collected by its employees, is done so with integrity and is kept secure and confidential, with accountability in the forefront of the organisation.

If you have any queries relating to the British Woodworking Federation GDPR policy, or you have any concerns about how personal data has been handled then please contact the British Woodworking Federation using the details provided below.

bwf@bwf.org.uk