

This policy and our supporting GDPR Procedure set out how BCM seek to protect personal data and ensure that individuals understand the rules governing the collection, use and sharing of their personal data to which BCM have access to.

We hold personal and sensitive data about our employees, clients, suppliers, consultants, stakeholders and other individuals for a variety of business purposes which all must adhere to and be in accordance with the General Data Protection Regulations (2018) and the Data Protection Act (2018). The regulations include the following rights for individuals around their personal data:

- The right to be informed of the personal data being held
- The right of access
- The right to certification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object to the processing of their data
- The right not to be subject to automated decision-making including profiling

The regulations place greater emphasis on processing both personal and sensitive data that companies must keep and to demonstrate their accountabilities. Personal data is any information relating to identifiable individuals such as name, home address, email, phone number or an ID number. Sensitive personal data is personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health conditions, drugs and alcohol tests and medication, criminal offences, or related proceedings – any use of sensitive data will be strictly controlled in accordance with this policy and supporting procedures.

Business Purposes:

BCM ensures that a designated BCM Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The purpose for which personal data may be used by BCM is categorised as - personal, administrative, financial, regulatory, payroll, sentinel scheme rules and business development. Business purposes include the following:

1. Compliance with our legal, regulatory and corporate governance obligations
2. Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
3. Ensuring BCM's other supporting policies are adhered to (such as policies covering email, social media and internet use)
4. Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting
5. Investigating complaints
6. Conducting HR related checks such as references, staff absences, training, sentinel compliance, monitoring medicals, declared medication, drugs and alcohol tests, monitoring staff conduct
7. Ensuring safe working practices and monitoring and managing employees' access to systems and facilities
8. Improving services

This Policy Statement and associated IMS procedures apply to all activities undertaken by BCM. All employees are required to comply with this policy. They will be briefed on this during the induction process and following any subsequent amendments. It will be accessible to all interested parties via SharePoint, noticeboards, the company website and is available on request.

The Directors of BCM are committed to this policy and are responsible for ensuring its arrangements are implemented and upheld. It will be reviewed annually and revised as often as may be deemed appropriate.

Shane O'Halloran
Managing Director
February 2020

Issue no.:	2	Date:	Feb 2020	Parent document:		Page 1 of 1
Document owner:				Project Filing location:		
Uncontrolled when downloaded or printed				Document control:		