PRIVACY AND DATA PROTECTION POLICY

1. INTRODUCTION

1.1 In our everyday business operations, our business makes use of a variety of data about identifiable individuals including data about.

- Current, past and prospective employees.
- Our service users and clients
- Supplier and subcontractors
- Other stakeholders.

1.2 In collecting and using this data, the business is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

1.3 The purpose of this policy is to set out the relevant legislation and to describe the steps our business is taking to ensure that it complies.

1.4 The control applies to all systems, people and processes that constitute the organisation's information systems, including directors, employees, suppliers and other third parties who have access to our business' systems.

1.5 The following policies and procedures are relevant to this document

- Data Protection impact assessment process
- Personal Data Mapping Procedure
- GDPR Roles, Responsibilities and Authorities
- Records, Retention and Protection Policy
-

2. PRIVACY AND PERSONAL DATA PROTECTION POLICY

2.1 The General Data Protection Regulation 679/2016 (GDPR) is one of the most significant pieces of legislation affecting the way the business carries out information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of people in the European Union. Its is the business' policy to ensure that our compliance with GDPR and other relevant legislation is clear and demonstrable at all times.

2.2 There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

- Personal date is defined as – Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person;
- Processing means – Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- Controller means – The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and the means of the processing of personal data; where the purpose and means of such processing are determined Union or member of state law, the controller or the specific criteria for its nomination may be provided by Union or member state law.

3. PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

3.1 There are a number of fundamental principles upon which the GDPR is based. These are as follows

3.1.1 Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")
- Collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be incompatible with the initial purposes ("purpose limitation");
- Adequate, relevant, and limited to what is necessary in relation to the purpose for which they are processed ("data minimisation")
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they personal data are processed; personal data may be stored for long periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures by this Regulation in order to safeguard the rights and freedoms of data subject ("storage limitations")
- Processed in a manner that ensures appropriate security of the personal data, including protection unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")
- The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 "(accountability")

4. RIGHTS OF THE INDIVIDUAL

4.1 The data subject also has rights under the GDPR, these consist of:

- 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.

4.2 Each of these rights are supported by appropriate procedures within the business, that allow the required action to be taken within the timescales stated in the GDPR.

4.3 These timescales are shown in table 1 below:

DATA SUBJECT REQUEST	TIMESCALES
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling	Not Specified

Table 1 – Timescales for data subject requests

5. CONSENT

5.1 Unless it is necessary for a reason allowable in the GDPR, explicit consent must be obtained from a data subject to collect and process their data. In case of children below the age of 16 parental consent must be obtained. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights with regards to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

5.2 If the personal data are not obtained directly from the data subject, then this information must be provided within a reasonable period after the data are obtained and within one month.

6. PRIVACY BY DESIGN

6.1 The business has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

6.2 The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purpose.
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data.
- . What controls are necessary to address the identified risks and demonstrate compliance with legislation.

6.3 Use of techniques such as minimization and pseudonymisation should be considered where applicable and appropriate.

7. TRANSFER OF PERSONAL DATA

7.1 Transfer of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

7.2 Intra-group international data transfers must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

8. DATA PROTECTION OFFICER

8.1 A defined role for Data Protection Officer (DPO) is required under the GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large-scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can with er be an in-house resource or outsourced to an appropriate service provider.

8.2 A2B Contract Cars Limited does have an in-house Data Protection Officer.

9. BREACH NOTIFICATION

9.1 It is our business' policy to be fair and proportionate when considering the actions to be take to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant Data Protection Authority (DPA) will be informed within 72 hours. This will be managed in accordance with our Information Security Incident Response Procedure which sets out the overall process of handling information security incidents.

9.2 Under the GDPR the relevant DPA has the authority to impose a range of fines for up to four percent of annual worldwide turnover for infringements of the regulations.

10. ADDRESSING COMPLIANCE TO GDPR

10.1 The following actions are undertaken to ensure that our business complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear unambiguous
- All staff involved in handling personal data understand their responsibilities for the following good data protection practice.
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changes to systems and processes.
- The following documentation of processing activities are recorded
    - Organisation name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Personal data retention schedules
    - Relevant technical and organisational controls in place

11. REVIEW

11.1 This policy is and will be reviewed on a regular basis but a least every 12 months after the date of last review as part of our management review process of the Data Protection Program.