GENERAL DATA PROTECTION REGULATIONS POLICY

1. Introduction

Alltask Ltd (Alltask) processes the personal data of living individuals such as its staff, contractors and customers. This processing is regulated by the Data Protection Act 1998 (DPA) and from May 2018 the General Data Protection Regulation (GDPR). The UK's regulator for the DPA and GDPR is the Information Commissioner's Office (ICO).

Alltask Ltd is registered as a Data Controller with the ICO 1 and is responsible for compliance with the GDPR and DPA.

1.1 Key Definitions

This DPA and GDPR contain a number of key definitions which are referenced in this policy such as 'personal data', 'processing' and 'Data Controller'. Those definitions are set out in **Annex A**.

1.2 Purpose and Objectives of Policy

This policy sets out the Alltask's commitment to comply with the Data Protection Act 1998 ('DPA'), and from May 2018, the General Data Protection Regulation ('the GDPR').

1.3 Scope and Status of the Policy

This policy applies to all staff and others who use or process any personal data. This policy applies regardless of where personal data is held and or the equipment used if the processing is for Alltask's purposes. Further, the policy applies to all personal data, sensitive personal data or special category data held in any form whether manual paper records or electronic records.

1 You can view our registration with the ICO by typing Alltask Limited into the search function accessible
via the following link: https://ico.org.uk/about-the-ico/what-we-do/register-of-data- controllers/

2. Roles and Responsibilities

Board of Directors

The Board of Directors is responsible for approval of the Policy.

Executive Group

The Executive Group is responsible for strategic level implementation of the policy, oversight of compliance with the policy and reporting identified risks to the Board.

IT Services

IT are available for providing advice, support and guidance in relation to day to-day data protection matters.

All staff

All staff, including permanent staff, fixed term contractors and temporary workers must comply with this Policy, the DPA and from May 2018 the GDPR whenever processing personal data held by Alltask Ltd.

Contractors and Consultants

Third parties such as consultants, contractors or agents, undertaking work on behalf of Alltask involving personal data, must adhere to Alltask's Data Protection Policy and comply with the DPA and from May 2018, the GDPR. Provision will be made in contracts with external providers to ensure compliance with this Policy, the DPA and GDPR.

3. Compliance with the DPA and GDPR

3.1 Awareness & Capability

Alltask will implement, and monitor annual completion of, mandatory Data Protection training for all staff. The content of that training will be reviewed annually.

3.2 Privacy By Design

Alltask will implement a Privacy By Design Approach to processing personal data through integrating Privacy Impact Assessments into business processes and projects.

3.3 Security

Alltask will protect the security of personal data by maintaining, and monitoring compliance with Alltask's Data protection Policy.

3.4 Record Keeping & Retention

Alltask will maintain a Records Retention and Disposal Schedule setting the periods for which records containing personal data are to be retained.

3.5 External Contractors and International Transfers

Alltask will enter into legally binding contracts with external bodies where those bodies are engaged to process personal data on our behalf. Alltask will implement adequacy arrangements where transferring any personal data outside of the European Union.

3.6 Other Third-Party Access

Alltask will only disclose personal data to third parties such as the police, central government etc. where there is a lawful basis for doing so and appropriate arrangements are in place with those parties.

3.7 Internal Sharing

Alltask will seek to ensure that personal data is only shared across different teams, divisions or faculties where those areas have a business need for accessing that data**.**

4. Data Subjects Rights

Alltask will comply with requests from an individual to exercise their rights under the DPA, and from 25 May 2018, the GDPR. All individuals have the right to be informed what information Alltask holds about them and to request copies of that information. This is known as a Subject Access Request. Any individual wishing to submit a Subject Access Request should send an email to datarequest@alltask.co.uk or call 01634 298000.

Under the DPA and GDPR, individuals also have the following rights in relation to their personal data:

- The right to request their personal data is rectified if inaccurate
- The right to request erasure of their personal data
- The right to request that the processing of their personal data is restricted
- The right of portability in relation to their personal data
- The right to object to the processing of their personal data
- The right to object to processing which involves automated decision making or profiling.

Individuals who wish to exercise the above rights should contact the datarequest@alltask.co.uk. Individuals should submit their request in writing and specify exactly what personal data and/or processing they are referring to and which right they wish to exercise.

Any staff member who receives a Subject Access Request or a request from an individual to exercise the above rights under the DPA and GDPR must be forwarded datarequest@alltask.co.uk immediately. All staff are responsible for helping to ensure that Alltask can comply with an individual's request under the DPA and GDPR within the statutory timescales.

5. Own Personal Data

All staff are responsible for checking that information they provide to the Alltask in connection with their employment is accurate and up to date. Any changes to personal data provided (e.g. change of address) must be promptly notified, in writing, to Alltask HR. Alltask cannot be held responsible for errors unless the member of staff has properly informed the Alltask about them.

6. Personal Data Breaches

Alltask will respond promptly to any identified personal data breaches and thoroughly investigate those incidents to ascertain whether;

- The breach should or must be reported to the ICO
- Data subjects should or must be made aware of the breach; and
- It is necessary to amend processes or introduce new measures to mitigate against any further breaches.

Any staff member who knows or suspect an actual or potential personal data breach has occurred must immediately notify your line manager or email databreach@alltask.co.uk. All staff are responsible for fully engaging in relation to the investigation of a personal data breach.

7. Compliance

Compliance with this Policy, the DPA and from May 2018, the GDPR is the responsibility of all members of staff. Employees must comply with the rules and procedures made by Alltask.

Any breach of the policy by a member of staff may result in disciplinary action or access to the Alltask facilities being withdrawn. Serious or deliberate breaches of the DPA can result in a criminal prosecution.

Any breach of the GDPR by Alltask may result in a substantial fine or actions imposed upon the Company by the ICO.

8. Further Information

Questions about the interpretation or operation of this policy, or any individual who considers that the Policy has not been followed in respect of personal data about themselves should be taken up in the first instance with your line manager.

Further information about the Data Protection Act 1998 and the GDPR can be found on the Information Commissioner's Office (ICO website).

Signed: January 2020

Daniel Finchal

CEO

Annex A Key Definitions

1. 'Personal Data' means data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual. Under the GDPR, the definition of personal data will explicitly extend to IP addresses.

2. 'Sensitive Personal Data' means information about an individual's ethnicity, political opinions, their religious beliefs or other beliefs of a similar nature, membership of a trade union, disability, sexual orientation, the commission or alleged commission by them of any criminal offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings of the sentence of any court in such proceedings.

3. Under the GDPR, the term 'sensitive personal data' will be replaced by the definition special category data which means any personal data information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and their genetic or biometric data.

4. Processing; means any operations or set of operations which is performed on personal data whether or not by automated means such as collection, use, disclosure or storage of personal data etc.

5. 'Data Controller means the organisation which, either alone or jointly with another organisation, determines the manner and purpose of the processing of personal data. The Data Controller is responsible for compliance with the DPA and GDPR.

6. 'Data Processor' means an organisation (such as a contractor) which processes personal data on behalf of a Data Controller.

7. 'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.