Dumarey Flybrid HR Procedures

DATA PROTECTION & GDPR COMPLIANCE POLICY

Introduction

Dumarey Flybrid Limited is committed to data protection by default and by design and supports the data protection rights of all those with whom it works, including, but not limited to, job applicants, employees, customers and suppliers. This policy sets out the accountability and responsibilities of the Company and its employees to comply fully with the provisions of the UK General Data Protection Regulation ("the UK GDPR") and the Data Protection Act 2018 ("the DPA") and recognises that handling personal data appropriately and in compliance with data protection legislation enhances trust, is the right thing to do and protects the Company's relationship with all its stakeholders.

The Company holds and processes personal data about individuals such as employees, job applicants, customers and others, defined as 'data subjects' by the law. Such data must only be processed in accordance with the UK GDPR and the DPA.

This policy covers the following areas:

- Purpose and scope of the policy
- Responsibilities under the policy
- Data protection by design and default
- Responsibility of management and data users
- Data subject rights
- Internal data sharing
- Transfers of personal data outside the EEA
- Direct marketing
- Data protection training
- Data protection breaches

Purpose and Scope of policy

This policy sets out the responsibilities of the Company and its employees to comply fully with the provisions of the UK GDPR and the DPA.

This policy applies to all employees in all cases where the Company or its employees are the data controller or a data processor of personal data. The policy applies in these cases regardless of who created the data, where it is held, or the ownership of the equipment used. Any failure to follow the policy can therefore result in disciplinary proceedings.

Responsibilities under the policy

The Company as data controller has a corporate responsibility to implement and comply with data protection legislation. In determining the purposes for which, and the manner in which, personal data is processed, the Company must adhere to the six Data Protection Principles ("the Principles") as set out in the legislation.

This section will set out the main requirements for compliance.

Data security

All users of personal data within the Company must ensure that personal data is always held securely and not disclosed to any unauthorised third party either accidentally, negligently or intentionally.

Privacy notices

When the Company collects personal data from individuals, the requirement for 'fairness and transparency' must be adhered to. This means that the Company must provide data subjects with a 'privacy notice' to let them know how and for what purpose their personal data are processed. Any data processing must be consistent or compatible with that purpose.

Conditions of processing/lawfulness

In order to meet the 'lawfulness' requirement, processing personal data must meet at least one the following conditions:

1. The data subject has given consent.
2. The processing is required due to a contract.
3. It is necessary due to a legal obligation.
4. It is necessary to protect someone's vital interests (i.e. life or death situation).
5. It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. It is necessary for the legitimate interests of the controller or a third party.

For special categories of personal data, at least one of the following conditions must be met:

1. The data subject has given explicit consent.
2. The processing is necessary for the purposes of employment, social security and social protection law.
3. The processing is necessary to protect someone's vital interests.
4. The processing is carried out by a not-for-profit body.
5. The processing is manifestly made public by the data subject
6. The processing is necessary for legal claims
7. The processing is necessary for reasons of substantial public interest.
8. The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services.
9. The processing is necessary for public health
10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards

Data retention

Personal data must not be kept longer than necessary for the purposes for which it was originally collected. This applies to all personal data, whether held on core systems, local PCs, laptops or mobile devices or held on paper. If the data is no longer required, it must be securely destroyed or deleted. The Company's Privacy Notices give an indication as to how long personal data must be kept and are based on both legal and business requirements:

Data protection by design and default

Under the UK GDPR and the DPA, the Company has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the potential negative impact processing can have on the data subjects' privacy.
The Company employs virus scanning, firewalls and regular software and malware updates to secure the data we hold. All laptops and systems are password protected and users are trained at induction in the contents of this policy and the importance of information security.

Anonymisation and pseudonymisation

Mechanisms of reducing risks associated with handling personal data are to apply anonymisation or pseudonymisation. Wherever possible, personal data must be anonymised or, where that is not possible, pseudonymised.

Responsibilities of management and data users

Line Managers have a responsibility to ensure compliance with the UK GDPR, the DPA and this policy, and to develop and encourage good information handling practices within their areas of responsibility. All users of personal data within the Company have a responsibility to ensure that they process the data in accordance with the Principles and the other conditions set down in the legislation.

Data subject rights

The UK GDPR and the DPA contain eight data subject rights the Company must comply with – the rights to information, subject access, to rectification, to object, to erasure, to portability, to restrict processing and in relation to automated decision-making and profiling.

Subject access requests and the right to data portability

Individuals have the right to request to see or receive copies of any information the Company holds about them, and in certain circumstances to have that data provided in a structured, commonly used and machine-readable format so it can be forwarded to another data controller. The Company must respond to these requests within four weeks.

It is a personal criminal offence to delete relevant personal data after a subject access request has been received.

Right to erasure, to restrict processing, to rectification and to object

In certain circumstances data subjects have the right to have their data erased. This only applies

- where the data is no longer required for the purpose for which it was originally collected, or
    - where the data subject withdraws consent, or
- where the data is being processed unlawfully.

In some circumstances, data subjects may not wish to have their data erased but rather have any further processing restricted.

If personal data is inaccurate, data subjects have the right to require the Company to rectify inaccuracies. In some circumstances, if personal data are incomplete, the data subject can also require the controller to complete the data, or to record a supplementary statement.

Data subjects have the right to object to specific types of processing such as processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right.

Individuals receiving any of these requests should not act to respond but instead should contact the HR Manager immediately.

Rights in relation to automated decision making and profiling

In the case of automated decision making and profiling that may have significant effects on data subjects, they have the right to either have the decision reviewed by a human being or to not be subject to this type of decision making at all. These requests must be forwarded to the HR Manager immediately.

Data sharing

When personal data is transferred internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected

When personal data is transferred externally, a legal basis must be determined and a data sharing agreement between the Company and the third party must be signed, unless disclosure is required by law, such as certain requests from the Department for Work and Pensions or Inland Revenue, or the third party requires the data for law enforcement purposes.

Transfers of personal data outside the EEA

Personal data can only be transferred out of the UK when there are safeguards in place to ensure an adequate level of protection for the data.

Any transfer of personal data out with the EEA that uses the Standard Contractual Clauses (SCCs) as a safeguard will need to be evaluated and authorised by the Managing Director.

Direct marketing

Direct marketing does not only cover the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals. For the Company, this will include notifications about events, selling goods or services. Marketing covers all forms of communications, such as contact by post, fax, telephone and electronic messages, whereby the use of electronic means such as emails and text messaging is governed by the Privacy and Electronic Communications Regulations 2003 (PECR). The Company must ensure that it always complies with relevant legislation every time it undertakes direct marketing and must cease all direct marketing activities if an individual requests it to stop.

Data protection training

Data protection briefings will take place for all employees as part of their induction programme and during weekly stand up meetings.

Data protection breaches

The Company is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The Company makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Any data protection incident must be brought to the attention of HR Manager who will investigate and decide if the incident constitutes a data protection breach. If a reportable data protection breach occurs, the Company is required to notify the Information Commissioner's Office as soon as possible, and not later than 72 hours after becoming aware of it.

Signed: 

Tobias Knichel
Managing Director
January 2024

Document Name	Owner / Updated by:	Changes &Date of Release	Next Review
Data Protection & GDPR Compliance Policy	E Hart - HR	Created 06/03/2023	Jan 2024
Data protection & GDPR Compliance Policy	E Hart- HR	Dumarey Rebrand & review 03/01/24	Jan 2025