Special Personal Data. The Unity Partnership Ltd

Additional Data Protection Policy

Version 5.0

May 2020

Unitypartnership

Contents

1 Objectives

1.1 We recognise the need for legal compliance and accountability and endorse the importance of the integrity, availability, confidentiality and security arrangements to safeguard personal data. We also recognise that there are times that personal data is shared with, and/or received from other organisations and that this needs to be in accordance with the law.

1.2 This policy sets out the key data protection obligations and accountability to which we are fully committed in relation to:

1.3 General processing

- The processing of special categories of personal data (including criminal conviction and offence data) within the scope of the General Data Protection Regulation (GDPR).

2 Scope

2.1 This policy covers all aspects of handling special category data and sensitive processing regardless of age, format, systems and processes used, developed and managed by us. This includes processing by persons directly employed by us and any other persons instructed under contract to act on our behalf.

2.2 Special category data means personal data revealing:

- racial or ethnic origin;
- religious or philosophical beliefs;
- political opinions or trade-union membership;
- the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person;
- data concerning health
- a person's sexual life or sexual orientation
- criminal conviction or offence data.

2.3 The purpose of this policy is to set out the additional safeguards that apply to these categories of data and the controls in place to ensure that it is collected, used and shared appropriately and responsibly.

2.4 In order to fulfil our statutory and operational obligations, it will be necessary to collect, use, receive and share personal data that because of its sensitive nature requires careful handling and protection. We will endeavour to strike the right balance between our need as a data controller to act in the public interest while at the same time respecting the rights and freedoms of the individuals to whom the personal data relates.

2.5 This policy reflects the commitment to data protection compliance and the privacy elements of human rights legislation. In particular this includes:

- the EU General Data Protection Regulation 2016 (GDPR) as supplemented by the Data Protection Act 2018 (DPA 2018)

- the European Convention of Human Rights 1950 and UK Human Rights Act 1998.

3 Policy

3.1 Data Protection Officer (DPO)

We will appoint a data protection officer who will be the key contact for the provision of independent advice for all matters relating to data protection compliance. The DPO will be responsible for ensuring that we are appropriately registered with the Information Commissioner's Office (ICO) and facilitating the mandatory Record of Processing Activities (ROPA), to be made available to the ICO upon demand.

3.2 Data Protection Principles

There are 6 data protection principles and these provide the framework for ensuring that personal data is:

(a) processed lawfully, fairly and in a transparent manner

This means identifying the legal power, duty or function underpinning the reason for the processing and the appropriate data protection condition(s) relied on.

It also means that privacy notices must communicate key information, including why and what types of data are to be collected, used and shared in order to satisfy transparency requirements.

(b) processed for an explicit and specific purpose and not processed for other incompatible purposes

This means personal data collected for one purpose cannot be used for unrelated purposes unless the law expressly permits this. An exception applies for scientific/historical/statistical research and archiving in the public interest.

(c) adequate, relevant and limited to what is necessary for the purpose

This principle aims to ensure that only the minimum necessary personal data is collected and used.

(d) accurate and, where necessary, kept up to date; ensuring that personal data that are inaccurate, are erased or rectified without delay

This principle requires those responsible for the processing to ensure that the personal data is accurate and up to date, including notifying recipients so that any errors are corrected.

(e) keep no longer than necessary in identifiable form

This principle requires that personal data is not stored in identifiable form for longer than is necessary. An exception applies for scientific/historical/statistical research and archiving in the public interest.

(f) protection of the personal data using appropriate technical or organisational measures

This principle requires those responsible, including those instructed under contract, to ensure that personal data is protected from unauthorised access and misuse and that the technical and organisational measures take account of the harm that could be caused if control of the data were to be lost or compromised.

3.3 Accountability Obligation

In line with the accountability obligation, we are committed to observing and to demonstrating its compliance with all the data protection principles.

In relation to lawful processing, we will ensure that it identifies appropriate data protection conditions.

3.4 Data Privacy Impact Assessments (DPIA)

DPIAs are an important vehicle in ensuring that we integrate data protection by design and default into our technical systems and day to day business operations by embedding privacy risk considerations into new and changes to systems and business processes. These assessments must take place where there is a high risk to the privacy rights and freedoms of a data subject. Examples where these are likely to be required include but are not limited to new systems and processes, new or different uses of personal data. Where a high risk is identified the DPO must be consulted before any new or changed processing is introduced to ensure adequate risk mitigation measures are implemented. Where risks are high and not adequately mitigated a referral to the ICO must be made.

3.5 Data Collection, Use and Disclosure

We collect personal data directly from service users and individuals as well as receiving it from or sharing it with relevant third parties such as public sector and regulatory organisations, private and voluntary sector organisations, complainants etc.

3.6 As a data controller we are committed to

- only handling personal data lawfully and only to the extent it is necessary to do so

- not unnecessarily relying on consent where an alternative legal basis is available for processing personal data. If consent is the appropriate lawful basis, we acknowledge that valid consent must be freely given, fully informed and capable of being withdrawn. Where an individual is unable due to age, capacity or other reasons to give consent directly, consent will be sought from an appropriate person, e.g. parent, guardian, legal representative, etc.
- only sending promotional or marketing material with consent/or existing business relationship
- providing data subjects with privacy notices that explain why the personal data is required and how individuals can exercise their personal data rights
- protecting personal data but in the event of a personal data security breach, resulting in a high risk to the data subject(s) undertake to notify individuals and/or the ICO as appropriate
- assisting individuals to exercise their personal data rights, and to responding within the statutory time limits and providing a complaints process
- ensuring personal data is subject to appropriate retention and security controls taking into account the purpose of processing, the nature of the data and the information risks
- ensuring that when sharing and disclosing personal data this is undertaken within the parameters of the law to prevent misuse, unauthorised access to personal data. A record will be kept and where appropriate information sharing agreements (ISA) will be developed in line with the ICO Data Sharing Code of Practice. Where the sharing involves a joint controller relationship, the ISA will identify the lead controller responsible for specified processing activities and for managing individual rights. Where appropriate, DPIA's will be undertaken in advance of the sharing/disclosure
- ensuring our Records of Processing Activities (RoPA) are maintained
- ensuring that processing of personal data within our supply chains includes the contractual clauses required by law and that processing is only undertaken in accordance with our instructions
- not transferring personal data outside of the European Economic Area (EAA) to countries with lower data protection standards, unless the appropriate safeguards and controls are in place, ie, a decision by the EU that the country has 'adequate' data protection legislation, that a company in the US is signatory to the EU/US privacy shield, or model contract clauses in place, or the law prescribes this in defined circumstances
- co-operating and providing information to the ICO and other regulatory bodies in pursuance of any investigation or enforcement action.

3.7 Offences: The data protection legislation contains specific offences. It is an offence:

3.7.1 for a person knowingly or recklessly, without the consent of the data controller to:

- obtain or disclose personal data;

- procure the disclosure of personal data to another person;
- retain it without the consent of the original data controller;
- offer to sell, sell or buy the personal data obtained.

3.7.2 for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller, or to knowingly or recklessly handle such data.

3.7.3 to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the data subject making the request for access or portability would have been entitled to receive.

3.7.4 to require a data subject to provide or give access to information obtained via data subject access in relation to health, conviction/caution records for the purpose of recruitment, continued employment, in connection with provision of goods and service to the public. In summary, a data subject should not be obliged to make a data subject access request for this type of information as a condition/implied condition of employment or contract.

3.7.5 to intentionally obstruct or give false information to the ICO in the exercise of its powers under information notices and/or warrants.

4 Assessment and Monitoring

4.1 An assessment of compliance with requirements will be undertaken in order to provide:

- Assurance
- Gap analysis of policy and practice
- Examples of best practice
- Improvement and training plans

4.2 Reports will be submitted to Senior Management.

5 Responsibilities and Approvals

The Leadership Team is responsible for the approval of this Policy and ensuring that the necessary support and resources area available for the effective implementation of this Policy.

The Data Protection Officer is responsible for the review of this policy.

The Senior Information Risk Owner (SIROs) has overall ownership of the Information Risk Policy. The SIRO acts as champion for information risk to senior management and Board of Directors and is responsible for providing written advice to the Accounting Officer on the content of our Statement of Internal Control in regard to information risk. The SIRO is responsible for decisions in relation to any information issues or incidents.

The Information Manager and Information Management Team is responsible for specialist advice and support of all aspects of Information and Records Management and Governance.

Employees whether permanent, temporary or contracted, including students, contractors and volunteers are responsible for ensuring they are aware of the data protection legislation requirements and for ensuring they comply with these on a day-to-day basis. Where necessary advice, assistance and training should be sought. Any breach of this policy could result in disciplinary action or could constitute a criminal offence.

6 Authority for this Policy

6.1 This policy is owned by the Data Protection Officer on behalf of the Chief Operating Officer.

6.2 This delegation is to establish and approve internal policies dealing with all aspects of the management of our information security, records and information governance.

7 Policy Governance

7.1 The following table identifies who is Accountable and Responsible with regards to this policy. The following definitions apply:

- Accountable – the person who has ultimate accountability and authority for the policy.
- Responsible - the person(s) responsible for developing and implementing the policy.

Accountable	Managing Director
Responsible	SIRO

Special Personal Data – Additional Data Protection Policy			
Version	**Date**	**Author**	**Purpose/Changes**
0.1	March 2019	Barbara Mulvihill	Approved
0.2-3	May 2019	Karen Ollerenshaw	Unity specific
0.4	Oct 2019	Janine Taylor	Updates
1.0	May 2020	Joanna Gadd	Final