Policy: GDPR Data Protection Policy
Ref: P40 – F3.1

1. Scope

The Zacchaeus 200 Trust (Z2K) and its management and Board of Trustees, with a registered address at Fourth Floor, 79-80 Petty France, London SW1H 9EX are committed to being fully compliant with all applicable UK and EU data protection legislation in respect of personal data, as well to safeguarding the "rights and freedoms" of persons whose information Z2K collects pursuant to the General Data Protection Regulation ("GDPR") through the use of Salesforce, Office 365, Formstack, Box.Com, Z2K-owned computer equipment ("CRMs"), which is developed, implemented, maintained and periodically reviewed and amended by Z2K's Board of Directors.

The CRMs shall take into consideration the following: organisational structure, management responsibility, jurisdiction and geographical location and may comprise of a defined part of Z2K or Z2K as a whole.

2. Objectives

Z2K's objectives for the CRMs are as follows:

1. To enable Z2K to meet its personal data obligations in relation to how personal information is managed;

2. To support Z2K's objectives;

3. To set appropriate systems and controls according to Z2K's risk appetite;

4. To ensure that Z2K is compliant with all applicable obligations, whether statutory, regulatory, contractual and/or professional; and

5. To safeguard personnel and stakeholder interests.

3. Good practice

Z2K shall ensure compliance with data protection legislation and good practice, by at all times:

1. Processing personal information only when to do so is absolutely necessary for organisational purposes;

2. Ensuring that the least possible amount of personal data is collected, and that personal data is never processed unduly;

3. Informing individuals of how their personal data is or will be used and by whom;

4. Processing only pertinent and adequate personal data;

5. Processing personal data in a lawful and fair manner;

6. Keeping a record of the various categories of personal data processed, e.g. employment records in the data inventory schedule;

7. Ensuring that all current personal data that is kept is accurate and up to date on all non-archived or deleted (see retention policy) data;

8. Retaining personal data no longer than required by statute or regulatory body, or for organisational purposes which will be explained to the individual;

9. Giving individuals the right of 'subject access', as well as all other individual rights pertaining to their personal data;

10. Ensuring that all personal data is maintained securely;

11. Transferring personal data outside of the EU only in situations where it shall be appropriately secured;

12. Applying various statutory exemptions, where appropriate;

13. Implementing a CRMs, pursuant to this Policy;

14. Identifying stakeholders, both internal and external, and ascertaining their involvement within the operation of the CRMs; and

15. Identifying personnel that are responsible and accountable for the CRMs.

4. Notification

Z2K has registered with the Information Commissioner as a Data controller that engages in processing personal information of data subjects. Z2K has identified all of the personal data that it processes and recorded it in its P42.1_Data Inventory Schedule 92017-B.

The data controller shall retain a copy of all notifications made by Z2K to the Information Commissioner's Office ("ICO") and the ICO Notification Handbook shall be used as a record of all notifications made.

The ICO notification shall be reviewed on an annual basis on 9 July and the data controller shall be responsible for each annual review of the details of the notification, keeping in mind any changes to Z2K's activities. These changes shall be ascertained by reviewing the Data Inventory Schedule and the P44.2 GDPR Incident Register. Data protection impact assessments shall be used to ascertain any additional relevant requirements.

This policy applies to all employees of Z2K, including contractors and subcontractors. Breaches of the GDPR policy, shall be dealt with according to Z2K's P44 Reporting a Breach Policy & Procedure and Disciplinary Policy. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred to the relevant authorities.

All third parties working with or for Z2K who have or may have access to personal data are required to read, understand and fully comply with this policy at all times. All aforementioned third parties are required to enter into a data confidentiality agreement prior to accessing any personal data. The data protection obligations imposed by the confidentiality agreement shall be equally onerous as those to which Z2K has agreed to comply with. Z2K shall at all times have the right to audit any personal data accessed by third parties pursuant to the confidentiality agreement.

5. GDPR background

The purpose of the GDPR is to ensure the "rights and freedoms" of living individuals, and to protect their personal data by ensuring that it is never processed without their knowledge and, when possible, their consent.

6. Definitions (as per the GDPR)

- *Child* means anyone under the age of 16. It is only lawful to process the personal data of a child under the age of 13 upon receipt of consent from the child's parent or legal custodian.

- *Data controller* may be a natural or legal person, whether a public authority, agency or other body which, individually or jointly with others, is in charge of ascertaining the purposes and means by which personal data shall be processed. Where EU or Member State law predetermines the purposes and means of processing personal data, the data controller or, if appropriate, the specific criteria for selecting the data controller, may be provided for by EU or Member State law.

- *Data subject* refers to any living person who is the subject of personal data (see above for the definition of 'personal data') held by an organisation. A data subject must be identifiable by name, ID, address, online identifier or other factors such as physical, physiological, genetic, mental, economic or social.

- *Data subject consent* refers to any specific indication by the data subject that signifies consent to the processing of personal data. Consent may take place by way of a written or oral statement or by clear, unambiguous action and must be given freely at all times, without duress, with the data subject being properly informed.

- *Establishment* refers to the administrative head office of the 'data controller' in the EU, where the main decisions regarding the purpose of its data processing activities are made. 'Data controllers' based outside of the EU are required to appoint a representative within the jurisdiction in which they operate to act on its behalf and liaise with the relevant regulatory and supervisory authorities.

- *Filing system* refers to any personal data set which is accessible on the basis of certain benchmarks, or norms and can be centralised, decentralised or dispersed across various locations.

- *Personal data* – means any information relating to a data subject.

- *Personal data breach* refers to a security breach which results in the disclosure, alteration, destruction or loss of personal data, as well as unauthorised access to personal data that is stored, transmitted or processed by any other means, whether accidentally or unlawfully. All personal data breaches must be reported to relevant regulatory authority by the 'data controller' at all times, whereas the data subject need only be informed of a data breach when it is likely that the breach will have an adverse effect on his or her privacy or personal data.

- *Processing* refers to any action taken in relation to personal data, including but not limited to collection, adaptation or alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise.

- *Profiling* refers to any form of personal data processing that is automated, with the intention of assessing personal aspects of a data subject or analysing a data subject's employment performance, economic status, whereabouts, health, personal preferences and behaviour. The data subject has a right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling.

- *Special categories of personal data* refers to personal data covering such matters as racial or ethnic origin, beliefs - whether religious, political or philosophical - membership of a trade-union and data relating to genetics, biometric identification, health, sexual orientation and sex life.

- *Territorial scope* the GDPR applies to all EU based 'data controllers' who engage in the processing of data subjects**'** personal data as well as to 'data controllers' located outside of the EU that process data subjects**'** personal data so as to provide goods and services, or to monitor EU based data subject behaviour.

- *Third party* is a natural or legal person other than the data subject who is authorised to process personal data, whether a public authority, agency or other body controller, processor or any other person(s) under the direct authority of the controller or processor.

7. Responsibilities under the GDPR

Z2K is a Data controller pursuant to the GDPR.

Appointed employees of Z2K with managerial or supervisory responsibilities are responsible for ensuring that good personal data handling practices are developed, reviewed and encouraged within Z2K, as per their individual job descriptions.

Tanya Sutton, Office Manager, is the Data Protection Officer (DPO).

The position of DPO which involves the management of personal data within Z2K as well as compliance with the requirements of the DPA and demonstration of good practice protocol, is to be taken up by an appropriately qualified and experienced member of Z2K's management team.

The DPO reports to Z2K's Board of Directors and, amongst other things, is accountable for the development and implementation of the CRMs and for day-to-day compliance with this policy, both in terms of security and risk management. In addition, the DPO, is directly responsible for ensuring that Z2K is GDPR compliant and that managers and executive officers of Z2K are compliant in respect of data processing that occurs within their field of responsibility and/or oversight. An annual 'Letter of Assurance' will be presented to the Board confirming that the GDPR Policy has been satisfactorily complied with.

The DPO shall at all times be the first point of contact for any employees of Z2K who require guidance in relation to any aspect of data protection compliance.

The DPO is also responsible for other related GDPR procedures such as P43 Subject Access Request Policy 92017-C.~~.~~

It is not merely the DPO who is responsible for data protection, indeed all employees, volunteers, and sub-contractors of Z2K who process personal data are responsible for ensuring compliance with data protection laws and this is included in Z2K's training and development policy.

Employees, volunteers and sub-contractors of Z2K are personally responsible for ensuring that all personal data they have provided, and has been provided about them, to Z2K is accurate and up to date.

Risk Assessment

It is vital that Z2K is aware of all risks associated with personal data processing and it is via its risk assessment process that Z2K is able to assess the level of risk. Z2K is also required to carry out assessments of the personal data processing undertaken by other organisations on its behalf and to manage any identified risks, so as to mitigate the likelihood of potential non-compliance with this policy.

Where personal data processing is carried out by using new technologies, or when a high risk is identified in relation to the "rights and freedoms" of natural persons, Z2K is required to engage in a risk assessment of the potential impact. More than one risk may be addressed in a single assessment (also known as a 'Data Protection Impact Assessment' ("DPIA")).

If the outcome of a DPIA points to a high risk that Z2K's intended personal data processing could result in distress and/or may cause damage to data subjects, it is up to the DPO to decide whether Z2K ought to proceed and the matter should be escalated to him or her. In turn, the DPO may escalate the matter to the regulatory authority if significant concerns have been identified.

It is the role of the DPO to ensure that appropriate controls are in place to ensure that the risk level associated with personal data processing is kept to an acceptable level, as per the requirements of the GDPR and Z2K's documented risk acceptance criteria.

8. Principles of data protection

The principles of personal data processing are as follows:

1. All personal data must be processed lawfully and fairly at all times, as per Z2K's privacy notices.

2. Policies must also be transparent, meaning that Z2K must ensure that its personal data processing policies, as well as any specific information provided to a data subject, are readily available, easily accessible and clear, drafted using clear and plain language.

3. The data subject must be provided with the following information:

    a. *DPO* - the identity and contact details of the Data Protection Officer and any of its representatives;

    b. *Purpose* - the purpose or purposes and legal basis of processing;

c. *Storage period* - the length of time for which the data shall be stored;

d. *Rights* - confirmation of the existence of the following rights:
   i. Right to request access;
   ii. Right of rectification;
   iii. Right of erasure; and the
   iv. Right to raise an objection to the processing of the personal data;

e. *Categories* - the categories of personal data;

f. *Recipients* - the recipients and/or categories of recipients of personal data, if applicable;

g. *Location* - if the data controller intends to make a transfer of personal data to a third country and the levels of data protection provided for by the laws of that country, if applicable; and

h. *Further information* - any further information required by the data subject in order to ensure that the processing is fair and lawful.

4. Personal data may only be collected for specified, explicit and legitimate reasons. When personal data is obtained for specific purposes, it must only be used in relation to that purpose and cannot be different from the reasons formally notified to the Information Commissioner, as part of Z2K's GDPR ICO registration.

5. Personal data must be adequate, relevant and restricted to only what is required for processing. In relation to this, the DPO shall at all times:

   a. Ensure that personal data which is superfluous and not necessarily required for the purpose(s) for which it is obtained, is not collected;

   b. Oversee data collection forms, whether in hard-copy or electronic format;

   c. Carry out an annual review of all methods of data collection, checking that they are still appropriate, relevant and not excessive; and

   d. Securely delete or destroy any personal data that is collected in a manner that is excessive or unnecessary according to Z2K's GDPR policies.

6. Personal data must be accurate and up to date:

   a. Data should not be kept unless it is reasonable to assume its accuracy and data that is kept for long periods of time must be examined and amended, if necessary;

   b. All staff must receive training from the Office Manager to ensure they fully understand the importance of collecting and maintaining accurate personal data;

   c. Individuals are personally responsible for ensuring that the personal data held by Z2K is accurate and up to date. Z2K will assume that information submitted by individuals via data collection forms is accurate at the date of submission;

   d. All employees of Z2K are required to update the Office Manager as soon as reasonably possible of any changes to personal information, to ensure records are up to date at all times;

   e. The data controller must ensure that relevant and suitable additional steps are taken to ensure that personal data is accurate and up to date;

   f. The data controller shall, on an annual basis, carry out a review of all personal data controlled by Z2K, referring to the P42.1_Data Inventory schedule and ascertain whether any data is no longer required to be held in accordance with the guidelines of the ICO, arranging for that data to be deleted or destroyed in a safe manner.

   g. The data controller shall also ensure that where inaccurate or out-of-date personal data has been passed on to third parties, that the third parties are duly informed and instructed not to use the incorrect or out-of-date information as a means for making decisions about the data subject involved. The data controller shall also provide an update to the third party, correcting any inaccuracies in the personal data.

7. The form in which the personal data is stored must such that the data subject can only be identified when it is necessary to do so for processing purposes. The following principles apply:

   a. Personal data that is kept beyond the processing date must be either deleted, encrypted, pseudonymised or put beyond use and kept to an absolute minimum, to ensure the protection of the data subject's identity should a data breach incident occur;

b. Personal data must be retained according to the P42_Retention Requirements Policy 2017-F and P42.2 File Destruction Policy and must be destroyed or deleted in a secure manner as soon as the retention date has passed; and

c. Should any personal data be required to be retained beyond the retention period set out in the Records Retention Procedure, this may only be done with the express written approval of the data controller, which must be in line with data protection requirements.

8. The processing of personal data must always be carried out in a secure manner.

9. Personal data should not be processed in an unauthorised or unlawful manner, nor should it be accidentally lost or destroyed at any time and Z2K shall implement robust technical and organisational measures to ensure the safeguarding of personal data.

9. Security controls

Security controls are necessary to ensure that risks to personal data identified by Z2K are appropriately mitigated as much as possible to reduce the potential for damage or distress to data subjects whose personal data is being processed and are subject to regular audit and review.

Personal data shall not be transferred to a country outside of the EU unless the country provides appropriate protection of the data subject's 'rights and freedoms' in relation to the processing of personal data.

10. Adequacy of transfer

The following safeguards and exceptions are in place to ensure that data is not transferred to a country outside of the EU, with the transfer being off limits, unless one or more of the safeguards or exemptions listed below apply:

Safeguards

1. Assessing the adequacy of the transfer, by reference of the following:

- The nature of the personal data intended to be transferred;
- The country of origin and country of intended destination;
- The nature and duration of the personal data use;

- The legislative framework, codes of practice and international obligations of the data subject's country of residence; and
- (UK only) the security measures to be implemented in the country of intended destination in relation to the personal data.

2. Binding corporate rules

Z2K is free to implement approved binding corporate rules in relation to personal data transfer outside of the EU, however only with prior permission from the relevant regulatory body.

3. Model contract clauses

Z2K is free to implement model contract clauses in relation to personal data transfer outside of the EU and there will be an automatic recognition of adequacy of transfer, should the model contract clauses receive approval from the relevant regulatory body.

Exceptions

In the absence of an adequacy decision, including binding corporate rules and model contract clauses, no transfer of personal data to a third country may take place unless one of the following preconditions is satisfied:

1. Explicit consent has been provided by a fully informed data subject, who has been made aware of all possible risks involved in light of appropriate safeguards and an adequacy decision;

2. The personal data transfer is a prerequisite to the performance of a pre-existing contract between the data controller and the data subject or when the data subject requests that pre-contractual measures are implemented;

3. The personal data transfer is a prerequisite to the conclusion or performance of a pre-existing contract between the data controller and another person, whether natural or legal, if it is in the interest of the data subject;

4. The personal data transfer is in the public interest;

5. The personal data transfer is required for the creation, exercise or defense of legal claims;

6. The data subject is not capable of giving consent, whether due to physical or legal limitations or restrictions and the personal data transfer is necessary for the protection of the key interests of the data subject or of other persons;

7. The personal data transfer is made from an approved register, confirmed by EU or Member State law as having the intention of providing public information and which is open to consultation by the public or by an individual demonstrating a legitimate interest, but only so far as the legal requirements for consultation are fulfilled.

11. Accountability

According to the GDPR accountability principle, the Data Controller is responsible both for ensuring overall compliance with the GDPR and for demonstrating that each of its processes is compliant with the GDPR requirements. To this extent DPOs are required to:

- Maintain all relevant documentation regarding its processes and operations;
- Implement proportionate security measures;
- Carry out Data Processing Impact Assessments ("DPIAs");
- Comply with prior notification requirements;
- Seek the approval of relevant regulatory bodies; and

12. The rights of data subjects

Data subjects enjoy the following rights in relation to personal data that is processed and recorded:

1. The right to make access requests in respect of personal data that is held and disclosed;

2. The right to refuse personal data processing, when to do so is likely to result in damage or distress;

3. The right to refuse personal data processing, when it is for direct marketing purposes;

4. The right to be informed about the functioning of any decision-making processes that are automated which are likely to have a significant effect on the data subject;

5. The right not to solely be subject to any automated decision-making process;

6. The right to claim damages should they suffer any loss as a result of a breach of the provisions of the GDPR;

7. The right to take appropriate action in respect of the following: the rectification, blocking and erasure of personal data, as well as the destruction of any inaccurate personal data;

8. The right to request that the ICO carry out an assessment as to whether any of the provisions of the GDPR have been breached;

9. The right to be provided with personal data in a format that is structured, commonly used and machine-readable;

10. The right to request that his or her personal data is sent to another data controller; and

11. The right to refuse automated profiling without prior approval.

13. Data access requests

As far as possible, a completed subject access form (SAR) is to be given to the DPO who will review and process the request. The form is not a legal requirement, but Z2K would request one where possible for ease of recording.

14. Complaints

All complaints about the Z2K's processing of personal data may be lodged by a data subject directly with the Data Controller, by filling in the appropriate form providing details of the complaint. The data subject must be provided with the organisation's Privacy Policy at this stage.

Complaints may also be made by a data subject directly to the relevant regulatory body and Z2K hereby provides the relevant contact details: Tanya Sutton, Office Manager, email: tanyasutton@z2k.org, tel: 02072590801.

All complaints in relation to how a complaint has been handled and any appeals following the submission of a complaint shall be dealt with by the Data Controller and the data subject is required to submit a further complaint.

15. Consent

Consent to the processing of personal data by the data subject must be:

- Freely given and should never be given under duress, when the data subject is in an unfit state of mind or provided on the basis of misleading or false information;
- Explicit;
- Specific;
- A clear and unambiguous indication of the wishes of the data subject;
- Informed;
- Provided either in a statement or by unambiguous affirmative action;
- Demonstrated by active communication between the data controller and the data subject and must never inferred or implied by omission or a lack of response to communication;
- In relation to sensitive data, consent may only be provided in writing, unless there is an alternative legitimate basis for the processing of personal data.

Employees

Z2K will obtain consent to process personal and sensitive data when a new employee signs an employment contract or during induction programmes. Data subjects have the right to withdraw consent at any time and have been notified via the on-boarding procedure of Z2K.

Existing employees have been asked for their consent for Z2K to process their personal and sensitive data.

Employees have been notified of their rights under the GDPR within Z2K's employee handbook.

Employees have been notified of their obligations under the GDPR within Z2K's employee handbook.

Other data subjects – Clients, volunteers, supporters, donors

If using Consent as a condition to process data, Z2K will obtain Consent in accordance with the procedures outlined in the policy framework. Consent is considered to be a positive action on behalf of the data subject having read a clear, transparent and unambiguous privacy notice. It does not necessarily have to be a box that is ticked, it could be the completion of a form, or the supply of contact information. We understand that according to PECR consent does not have to be explicit. We will use our judgement to decide how to obtain consent in different

circumstances. However, we will always uphold the rights and freedoms of data subjects by always making it as easy to Opt-out as it ever was to Opt-in.

We mostly use Consent when promoting the aims and objectives of our organisation, Z2K. We reserve the right to use it wherever we believe a data subject has indicated their wishes and where we have collected the data for that particular purpose. We only use data for the purpose for which it was collected.

Parental consent

Parental or custodial consent is required if/when Z2K is a provider of online services to children, defined as being under the age of 16.

16. Data security

All employees of Z2K are personally responsible for keeping secure any personal data held by Z2K for which they are responsible. Under no circumstances may any personal data be disclosed to any third party unless Z2K has been provided express authorisation and has entered into a confidentiality agreement with the third party.

Accessing and storing personal data

Access to personal data shall only be granted to those who need it. This is determined by the Office Manager together with the line manager of the employee.

All personal data must be stored:

- In a locked room, the access to which is controlled; and/or
- In a locked cabinet, drawer or locker; and/or
- If in electronic format and stored on a computer, encrypted according to the corporate requirements set out in the Access Control Policy; and/or
- If in electronic format and stored on removable media, encrypted.

Before being granted access to any organisational data, all staff of Z2K would have been briefed on GDPR and confidentiality and have signed a Confidentiality Agreement.

Computer screens and terminals must not be visible to anyone other than staff of Z2K with the requisite authorisation.

No manual records may be accessed by unauthorised employees of Z2K and may not be removed from the business premises in the absence of explicit written authorisation. Manual records must be removed from secured archiving when access is no longer needed on a day-to-day basis.

All deletion of personal data must be carried out in accordance with P42_Z2K's Retention Requirements 92017-F and P42.2 File Destruction Policy. Manual records which have passed their retention date must be shredded and disposed of as 'confidential waste' and any removable or portable computer media such as hard drives must be destroyed securely.

Personal data that is processed 'off-site' must be processed by authorised Z2K staff, due to the increased risk of its loss, damage or theft.

17. Data access rights

Data subjects have the right to access all personal data in relation to them held by Z2K, whether as manual records or electronic format. Data subjects therefore may at any time request to have sight of confidential personal references held by Z2K as well as any personal data received by Z2K from third parties. To do so, a data subject must submit a P43.1_Subject Access Request, as per Subject Access Request SAR Form 92017-U.

18. Disclosure of data

Z2K must take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. This includes friends and family members of the data subject, governmental bodies and, in special circumstances, even the Police. All employees of Z2K are required to attend specific training in order to learn how to exercise due caution when requested to disclose personal data to a third party.

Disclosure is permitted by the GDPR without the consent of the data subject under certain circumstances, namely:

- In the interests of safeguarding national security;
- In the interests of crime prevention and detection which includes the apprehension and prosecution of offenders;
- In the interests of assessing or collecting a tax duty;
- In the interests of discharging various regulatory functions, including health and safety;
- In the interests of preventing serious harm occurring to a third party; and
- In the interests of protecting the vital interests of the data subject i.e. only in a life and death situation.

The data controller is responsible for handling all requests for the provision of data for these reasons and authorisation by the data controller shall only be granted with support of appropriate documentation.

19. Data retention and disposal

Z2K must not retain personal data for longer than is necessary and once an employee has left Z2K, it may no longer be necessary for Z2K to retain all of the personal data held in relation to that individual.

Personal data must be disposed of securely to ensure that the “rights and freedoms” of data subjects it protected at all times.

20. Document owner

The data controller is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated is available to all employees of Z2K on the ALL CURRENT POLICIES section of the file server.

This version of the policy document has been reviewed by a trustee and will be presented to Z2K's Board of Trustees at the next trustee meeting on the 18th November. This document is issued by the Chief Executive Officer ("CEO") on a version-controlled basis.

Name of CEO: Anela Anwar Date: September 2020