Envoy Partnership
Data Protection Policy

Contents

1. Introduction 3
2. Scope 3
3. Application of National Laws and Codes of Conduct 3
4. Principles for Processing Personal Data 4
   4.1. Lawfulness, Fairness and Transparency 4
   4.2. Purpose Limitation 4
   4.3. Data Minimisation 5
   4.4. Accuracy 5
   4.5. Storage Limitation 5
   4.6. Integrity and Confidentiality 5
   4.7. Restriction on Transfers 5
5. Legal Grounds for Data Processing 5
   5.1. Respondent Data 6
      5.1.1 Consent to Data Processing 6
      5.1.2 Data Processing for a Contractual Relationship 6
      5.1.3 Data Processing Pursuant to Legal Authorisation 6
      5.1.4 Data Processing Pursuant to Legitimate Interest 6
      5.1.5 Processing of Special Categories of Personal Data 6
      5.1.6 User Data and Internet 7
   5.2. Personal Data Provided by Clients 7
   5.3. Employee Data 7
      5.3.1 Data Processing for the Employment Relationship 7
      5.3.2 Data Processing Pursuant to Legal Authorisation 8
      5.3.3 Collective Agreements on Data Processing 8
      5.3.4 Consent to Data Processing 8
      5.3.5 Data Processing Pursuant to Legitimate Interest 8
      5.3.6 Processing of Special Categories of Personal Data 9
      5.3.7 Automated Decisions 9
      5.3.8 Telecommunications and Internet 9
      5.4. Marketing Contacts 9
6. Transmission of Personal Data 9
7. Outsourced/Third Party Data Processing 10
8. Rights of the Data Subject 11

Envoy Partnership Ltd.
Service address: 2nd floor, 1 Alfred Place, London WC1E 7EB
Tel: 0207 5588 062
Registered address: Chancery Station House, 31-33 High Holborn, London WC1V 6AX
Registered in England and Wales: Company number: 7641947 **VAT number: 125 8593 91**

9. Confidentiality of Processing 11
10. Privacy by Design and Default 12
11. Processing Security 12
12. Data Protection Audit 13
13. Data Protection Incidents 13
14. Responsibilities and Sanctions 13
14.1. Management 13
14.2. Data Protection Officers 14
15. Derogation 14
16. Glossary 14
Data Controller/Controller/Joint Controller 14
Data Users 14
Data processor or Processor 15
Data Subjects 15
Personal Data 15
Processing 15
Special categories of data (p/k/a personal sensitive data) 15
Anonymous Data 16
Pseudonymisation 16
PII or Personally Identifiable Information 16
PHI or Protected Health Information 17
PSI or Personal Sensitive Information 17
Policy Approval 17
Appendix 1: Data Storage 18
Appendix 2: Responsibilities for Data Protection 18
Appendix 3: Policy Implementation 19
Policy Implementation 19
Training 19
Subject Access Requests 19

1. Introduction

Envoy Partnership ("Envoy") is committed to international compliance with data protection laws, regulation and rules. Envoy's data protection policy ("Policy" or "Data Protection Policy") adopts the fundamental principles of the EU's General Data Protection Regulation ("GDPR") as the minimum standard to which Envoy, its employees and suppliers will have to adhere.

Envoy Partnership depends on the collection and analysis of information about living individuals ("Data Subjects") to carry out its research and consultancy work. Maintaining respondents' and the public's confidence requires that respondents do not suffer direct adverse consequences, risk or harm as a result of providing Envoy with their information or their Personal Data (for a definition and explanation of this term and other capitalised terms, please see the Glossary) being processed for Envoy's business purposes. The information may be obtained from any kind of individual or organisation.

To conduct its business, Envoy also needs to collect and process certain types of information about people with whom Envoy deals. These include current, past and prospective employees, suppliers, clients and others with whom it might communicate. In addition, Envoy may occasionally be required by law to process certain types of Personal Data to comply with the certain legal requirements.

This Policy describes the minimum standards of how Personal Data must be processed, collected, handled and stored to meet Envoy's data protection standards.

Data Users are obliged to comply with this Policy when processing Personal Data on Envoy's behalf. Any breach of this Policy may result in disciplinary action, up to and including dismissal from Envoy Partnership.

2. Scope

The Policy is applicable to all of Envoy Partnership's work. Within Envoy, this Policy will form the minimum standard to which all employees, subcontractors and suppliers have to adhere, regardless of whether GDPR directly applies to any specific activity or territory.

Everyone who works for Envoy has some responsibility for ensuring Personal Data are collected, stored and handled appropriately. It is everyone's responsibility that Personal Data are handled and processed in line with this Policy and its data protection principles.

Envoy also expects that its suppliers, subcontractors and vendors comply with the principles as set out herein.

3. Application of National Laws and Codes of Conduct

This Data Protection Policy adopts the internationally accepted privacy principles as enhanced by the GDPR. It is subsidiary to and supplements any applicable national legislation. The relevant national laws will take precedence if there is a conflict with this Policy or it has stricter requirements than this Policy. Any

registration, notification or reporting requirement for data processing under national laws must be observed. The contents of this Policy must also be observed in the absence of corresponding national legislation.

In the UK, Envoy adheres to the Market Research Society *Code of Conduct* in addition to this policy.[1]

4. Principles for Processing Personal Data

All Personal Data must be dealt with properly, irrespective of how they are collected, recorded and processed - whether on paper, in a computer file, database, or recorded on other material - and there are generally accepted principles to safeguard this, as set out in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, as well as relevant safeguards in various statutes across the world, including the GDPR.

Envoy regards the lawful and correct treatment of Personal Data and maintaining the confidence of those with whom it deals as a vital component of its business operations and is committed to act ethically and responsibly in respect of these Personal Data and to provide always a high degree of confidentiality and security.

To demonstrate these commitments, Envoy adheres to the principles relating to the processing of Personal Data found in the GDPR which are themselves an embodiment of the OECD principles. Envoy respects the following principles, which are explained in more detail later, concerning Personal Data and that they are:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.
- Not kept longer than necessary for the purpose.
- Processed in line with Data Subjects' rights.
- Secure.
- Not transferred to people or organisations situated in other countries without adequate protection.

4.1. Lawfulness, Fairness and Transparency

Personal Data must be processed and collected lawfully, fairly and in a transparent manner in relation to the Data Subject. Furthermore, Data Subjects must be informed of how his/her data are being handled. In general, Personal Data must be collected directly from the individual concerned. Where this is not the case the legal basis on which the processing is nevertheless justified must be documented.

4.2. Purpose Limitation

Personal Data must only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Subsequent changes to the purpose are

[1] https://www.mrs.org.uk/pdf/mrs%20code%20of%20conduct%202014.pdf

only possible to a limited extent and require substantiation and validation, in consultation with the DPO ("Data Protection Officer").

4.3. Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation for the purpose for which they are processed. It must be determined whether and to what extent the processing of Personal Data is necessary to achieve the purpose for which the processing is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized data must be used instead of Personal Data.

4.4. Accuracy

Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard for the purpose for which they are processed, are erased or rectified without delay.

4.5. Storage Limitation

Personal Data must not be retained in a form which permits identification of Data Subjects for longer than is necessary for the purpose for which the Personal Data are processed. Envoy will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. Envoy will take all reasonable steps to destroy, or erase from its systems, all Personal Data which are no longer required.

4.6. Integrity and Confidentiality

Personal Data must be processed in a manner that ensures appropriate security of the Personal Data from being revealed, disseminated, accessed or manipulated. Therefore, where methodologically possible and the expense is not disproportionate to the Data Subject's risks, pseudonymised data must be used for the processing – REMINDER: pseudonymised data remain and are Personal Data!

4.7. Restriction on Transfers

Personal Data must not be transferred to other countries that do not offer an adequate level of protection. This is particularly true of countries outside the European Economic Area (EEA). As part of its operations, Envoy stores some personal data outside of the UK, but within the European Economic Area. See *Appendix 1: Data Storage*.

5. Legal Grounds for Data Processing

Envoy will be collecting, processing and using Personal Data only under the following legal bases, always provided that such legal basis exists under applicable national law. One of these legal bases is also required if the purpose of collecting, processing and using the Personal Data is to be changed from the original purpose, unless there is clear compatibility between the original purpose and the new purpose. See also paragraph 4.2 and any potential additional compliance requirements.

5.1. Respondent Data

Respondents are the most common Data Subjects in Envoy's business. Consequently, the correct treatment of their Personal Data is at the heart of Envoy's business.

5.1.1 Consent to Data Processing

Personal Data can be processed following consent by the Data Subject. Before giving consent, the Data Subject must be informed in accordance with the transparency principle as set out under paragraph 4.1. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone surveys, consent can be given verbally. In all cases, the granting of consent must be documented.

Any consent will only be valid if it constitutes a freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which it giving a statement or by a clear affirmative action, signifies agreement to the processing of the Personal Data relating to him/her.

5.1.2 Data Processing for a Contractual Relationship

Apart from consent, their Personal Data may be processed where this is necessary in the context of a contract to which such Data Subjects is a party, to fulfil relevant obligations and rights. This applies also where such processing in necessary in order to establish or terminate a contract. This applies in particular to respondents (including mystery shoppers) in the sign up to the Envoy Partnership panels.

Some countries see the entering into a contract as a form of consent.

5.1.3 Data Processing Pursuant to Legal Authorisation

The processing of Personal Data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant statutory provisions.

5.1.4 Data Processing Pursuant to Legitimate Interest

Personal Data can also be processed if it is necessary for the legitimate interests of Envoy Partnership and where national legislation provides for this basis (e.g. GDPR Article 6(1)(f)). The legal basis of legitimate interest for processing is not recognised in every country, and relevant national legislation will take precedence. Generally, special categories of Personal Data may not be processed on the basis of legitimate interest. In any event, Personal Data may not be processed on the basis of a legitimate interest if, in the individual case, there is evidence that the interests of the Data Subject merit protection and that this protection takes precedence. Before Personal Data are processed on the legitimate interest basis, it is necessary to determine whether there is an interest that merits protection and a legitimate interest assessment (in the form of a Data Protection Impact Assessment with a particular focus on the legitimate interest) needs to be conducted by Envoy Partnership. Any such assessment has to be validated by the DPO.

5.1.5 Processing of Special Categories of Personal Data

Special categories of Personal Data can be processed only if the law requires this or the Data Subject has given his/her explicit consent. Special categories of Personal Data can also be processed if it is mandatory for asserting, exercising or defending legal claims. Within the EEA, special categories of Personal Data may also be processed for scientific and historical research and for statistical purposes (Article 9(2)(j)), subject to

appropriate additional measures. Before relying on these provisions, the advice of the DPO must be obtained.

5.1.6 User Data and Internet

If Personal Data are collected, processed and used on websites or in apps, the Data Subject must be informed of this in a privacy statement including, if applicable, information about cookies or similar technical measures. The privacy statement and any cookie information must be integrated so that it is easy to identify, directly accessible, easily understandable and consistently available by and for the Data Subject.

If use profiles (tracking) are created to evaluate the use of websites and apps, the Data Subjects must always be informed accordingly in the privacy statement. Tracking of Data Subjects online may only be effected if it is permitted under national law or upon explicit consent of the Data Subjects. Even if tracking uses a pseudonym for the Data Subject, the Data Subject should be given the chance to opt out in the privacy statement. In respect of online audience measurement without prior opt-in, Envoy also adheres to the principles promulgated by researchchoices.com.

If websites or apps can access Personal Data in an area restricted to registered users/respondents, the identification and authentication of the Data Subject must offer sufficient protection during access.

5.2. Personal Data Provided by Clients

Transmission of Personal Data to Envoy by its clients is a common occurrence. It usually happens to provide us with sample or to enhance existing sample. In respect of any Personal Data so received, Envoy will be the Processor and may only Process these Personal Data in accordance with the instructions agreed with or received from the client. These instructions may include restrictions on transfers to other parties or transfers to other countries as well as specific security requirements. Any such restrictions must be complied with. It is imperative that such instructions are documented in writing and agreed before any relevant contractual arrangements are accepted by Envoy, to ensure that Envoy is actually able to comply with any client specific restrictions or requirements.

Irrespective of any client requirements, any Personal Data provided by a client may only be:

a. Processed for the purpose they were provided for;
b. Not be kept for longer than is required for the purpose;
c. Subject to the same security requirements applicable to Envoy's own Personal Data.

5.3. Employee Data

5.3.1 Data Processing for the Employment Relationship

In employment relationships, Personal Data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicant's Personal Data can be processed. If the candidate is rejected his/her data must be deleted in observance with the required retention period unless the applicant has agreed to remain on file for a future selection process.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorised data processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws must be observed. In cases of doubt, consent must be obtained from the Data Subjects.

There must be legal authorisation to process Personal Data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee or the legitimate interest of the company.

5.3.2 Data Processing Pursuant to Legal Authorisation

Please see above at paragraph 5.1.3 for the further requirements.

5.3.3 Collective Agreements on Data Processing

If a data processing activity exceeds the purposes for fulfilling a contract, it may be permissible if authorised through a collective agreement between the employer and employee representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended further data-processing activity and must be drawn up within the parameters of national data protection and employment legislation.

5.3.4 Consent to Data Processing

Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Within the EU/European Economic Area, consent generally does not constitute a valid legal basis for the processing in the employment context as there is a legal presumption that such consent was not submitted voluntarily and any processing will have to rely on one of the other legal bases available. Involuntary consent is void. To the extent that consent is a valid basis for processing, please see above at paragraph 5.1.1 for the further requirements. A further complication is, that consent can normally be withdrawn, thereby preventing any further processing.

5.3.5 Data Processing Pursuant to Legitimate Interest

Personal Data may also be processed if it is necessary to enforce a legitimate interest of Envoy Partnership, where the applicable law allows for the processing of Personal Data based on a legitimate interest. Within the employment context, legitimate interests are generally of a legal or financial nature.

Please see above at paragraph 5.1.4 for the further requirements and limitations of legitimate interest.

Control or supervisory measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measures must also be examined before such measures are applied. The justified interests of the company in performing the control measure (e.g. compliance with internal company rules or security interests) must be weighed against any interest meriting protection that the employee affected by the measure may have in its exclusion and the measure cannot be performed unless found to be appropriate. The legitimate interests of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken by way of a legitimate interest assessment. Moreover, any additional requirements under national law (e.g. rights of codetermination for the employee representatives and information rights of the Data Subjects) must be taken into account.

5.3.6 Processing of Special Categories of Personal Data

Special categories of Personal Data can be processed only if the law requires this or the Data Subjects has given his/her explicit consent. These data can also be processed if it is mandatory for asserting, exercising or defending legal claims.

5.3.7 Automated Decisions

If Personal Data are processed automatically as part of the employment relationship and specific personal details are evaluated for decision making (e.g. as part of personnel selection process or the evaluation of scores), this automatic processing cannot be the sole basis for decisions that would have negative consequences or create significant problems for the affected employee. To avoid erroneous decisions, the automated process must ensure that a natural person evaluate the content of the situation, and that this evaluation is the basis for the decision. The Data Subjects must also be informed of the facts and results of automated individual decisions and the possibility to respond.

5.3.8 Telecommunications and Internet

Telephone equipment, email addresses, intranet and Internet along with internal social networks are provided by Envoy primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorised use for private purposes, the law on secrecy of telecommunications in the relevant national telecommunication laws must be observed, if applicable.

5.4. Marketing Contacts

Generally marketing contacts are no different than respondents in respect of the privacy protections accorded to them. Their contact details constitute Personal Data, even if they are business related. Only if the contact details are truly generic like “info@envoypartnership.com”, will they not fall under this Policy.

Marketing communications are often subject to specific legal requirements, particularly if they are sent electronically or made by phone.

It has to be assumed, that marketing contacts have not requested the marketing materials. In other words, the recipients have not asked to receive marketing communications from Envoy. To proceed legally, the conditions concerning legal basis, in particular, consent requirements set out in paragraph 5.1.1 apply here as well.

Exceptionally a 'soft opt-in' can be applied, if the below conditions are met:

- where the Data Subject’s details were obtained in the course of a sale or negotiations for a sale of Envoy services;
- where the messages are only marketing similar services; and
- where the person is given a simple opportunity to refuse marketing when their details are collected, and if they don't opt out at this point, are given a simple way to do so in all future messages.

6. Transmission of Personal Data

Transmission of Personal Data to recipients outside Envoy Partnership is subject to the authorisation requirements for processing Personal Data under paragraph 4.7 Restriction on Transfers. The data recipient

(including any sub-contractor) must be required to use the data only for the defined purposes. For external transfers the requirements of this paragraph and those of paragraph 7 Outsourced/Third Party Data Processing apply cumulative.

If Personal Data are transmitted to a recipient outside Envoy Partnership to a third country, this recipient must agree in writing to maintain a data protection level equivalent to this Data Protection Policy or as required under applicable law. For example, the GDPR stipulates various requirements that must be complied with, before any transfer may occur. This does not apply if transmission is based on a legal obligation. A legal obligation of this kind can be based on the laws of the domiciliary country of Envoy Partnership. In the alternative, the laws of the domiciliary country of Envoy Partnership may acknowledge the purpose of data transmission based on the legal obligations of a third country.

Where Personal Data are transmitted by third party (like a sample supplier) to Envoy Partnership, it must be ensured that the Personal Data can be used for the intended purpose. If Personal Data are transmitted by a third party to Envoy in error, the data will be permanently deleted by Envoy and the third party notified. If Personal Data are transmitted in a way that leads Envoy to believe that regulations and policies have not been fully followed by the third party, then Envoy will notify the third party and take any steps necessary to rectify this, including permanent deletion of the data.

7. Outsourced/Third Party Data Processing

In many cases Envoy is using external providers to process Personal Data. In these cases, an agreement on data processing on behalf of Envoy must be concluded with such provider. This can be done either by way of including appropriate provisions in the agreement governing the overall relationship with the provider or in a separate and specific document. In respect of processing on behalf of Envoy, the provider may only process the Personal Data as per the instructions from Envoy. When instructing a provider, the following requirements must be complied with:

- Where the Personal Data in question fall under paragraph 5.2 (client data), any relevant client requirements need to be passed down to the provider.
- The provider must be chosen based on its ability to cover the required technical and organisational protective measures and in line with Envoy supplier approval process.
- The provider must not subcontract the processing further without Envoy's prior written consent.
- The instructions must be placed in writing by way of an appropriate contract. The instructions on data processing and the responsibilities of Envoy and provider must be documented.
- Before the data processing begins, Envoy must be confident that the provider will comply with its duties. A provider can document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract. Envoy should retain the right to audit the provider's compliance.
- In the event of cross-border contract data processing, the relevant national requirements for disclosing Personal Data abroad must be met. In particular, the Personal Data from the European Economic Area can be processed in a third country only, if the provider can prove that it has a data protection standard equivalent to the GDPR and this Data Protection Policy. Suitable tools can be:

- an agreement based on EU standard contract clauses for contract data processing in third countries with the provider. Similar agreements will be required for any subcontractor of the provider.
- Participation of the provider in a certification system accredited by the EU for the provision of a sufficient data protection level.

8. Rights of the Data Subject

Every Data Subject has the following rights. Their request is to be handled immediately by Envoy Partnership and may not result in any disadvantage to the Data Subject. Where the relevant Personal Data are being processed by Envoy under paragraph 5.2 Personal Data Provided by Clients, the relevant client contract must be consulted in respect of any process to be followed and the client has to be informed about such request immediately.

- **Right of access:**
  - The Data Subjects may request information on which Personal Data relating to him/her have been stored, how the data were collected and for what purpose.
  - If Personal Data are transmitted to 3rd parties, information must be given about the identity of the recipient or the categories of recipients, including other Envoy companies.
- **Right to rectification:** If Personal Data are incorrect or incomplete, the Data Subject can demand that they are corrected or supplemented.
- **Right to withdraw consent:** Where the Personal Data are processed on the basis of Consent (see also the separate guidance on Consent), the Data Subjects can object to the processing at any time. These Personal Data must be blocked from the processing that has been objected to.
- **Right to erasure.** The Data Subject may request his or her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.
- **Right to object:** The Data Subjects generally has a right to object to his/her data being processed and this must be taken into account if the protection of his/her interest takes precedence over the interests of the data controller owing to the particular personal situation. This does not apply, if a legal provision requires that the Personal Data are data to be processed. The employment agreements with
- **Right to data portability**. The Data Subject has the right to request for the Personal Data provided by him/her to be made available to such Data Subject in an easily readable format, like a Word or Excel document.

9. Confidentiality of Processing

Personal Data are subject to data secrecy. Any unauthorised collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorised to carry out as part of his/her legitimate duties is un-authorised. The “need-to-know” principle applies. Employees may have access to Personal Data only as is appropriate for the type and scope of the

task in question. This requires a careful breakdown and separation, as well as in limitation, of roles and responsibilities.

Employees are forbidden to use Personal Data for their own private or commercial purposes, to disclose them to unauthorised persons, or to make them available in any other way. Supervisors must inform the employees at the start of the employment relationship about the obligation to maintain data secrecy. This obligation shall remain in force even after employment has ended. The employment agreements with Envoy staff must contain appropriate confidentiality obligations.

10. Privacy by Design and Default

Envoy will use a Privacy by Design and Default approach in all its work, but in particular when:

- building new IT systems for storing or accessing personal data;
- developing new applications or research approaches;
- embarking on a data sharing initiative; or
- using data for new purposes.

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. It is a key consideration in the early stages of any project, and then throughout its lifecycle.

Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust and will designing projects, processes, products or systems with privacy in mind from the outset

In respect of the examples given above, the required tool for compliance is conducting a Data Protection Impact Assessment.

11. Processing Security

Personal Data must be safeguarded from unauthorised access or disclosure (whether caused internally or externally), unlawful processing as well as accidental loss, modification or destruction. This applies regardless of whether the data is processed electronically or in paper form. Apart from securing existing Personal Data in line with Envoy's relevant policies, before the introduction of new methods of data processing, particular new IT systems or research approaches, technical or organisational measures to protect Personal Data must be defined and implemented. These measures must be based on the state of the art, the risk of processing and the need to protect the data.

These technical and organisational measures should be agreed in consultation with the DPO. The technical and organisational measures for protecting Personal Data are part of the Corporate Information Security management and must be adjusted continuously to technical development and advancement as well as organisational changes.

As a minimum, Envoy will process all Personal Data it holds in accordance with its Security Policy and take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

12. Data Protection Audit

Compliance with this Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the DPO. Various Envoy clients also have audit rights under their agreements with Envoy. The results of the data protection audits must be reported to the directors. On request, the results of data protection audits will be made available to the responsible data protection authorities.

13. Data Protection Incidents

All employees must inform the DPO immediately about cases of violations of this Data Protection Policy or other regulations on the protection of Personal Data. Any failure to address serious failings under this Policy can also be reported under the Envoy Whistle-blowing system.

In case of:

- improper transmission of Personal Data to 3rd parties;
- improper transmission of Personal Data across borders;
- improper access, including by third parties, to Personal Data, or
- loss of Personal Data (including then becoming public due to internal failures)

a data protection breach notification must be made immediately to ensure that a) any reporting duties under national law can be complied with, b) any affected client can be informed and c) any stakeholder communication can be managed. Any Data Protection breach will also constitute an information security incident under the IT Incident Management policy.

14. Responsibilities and Sanctions

See Appendix 2: Responsibilities for Data Protection for details of named individuals with specific responsibilities for Data Protection

14.1. Management

Management are responsible for ensuring that organisational, HR and technical measures are in place so that any data processing is carried out in accordance with these data protection requirements.

Compliance with these requirements is also the responsibility of the relevant employees.

Improper processing of Personal Data, or other violations of the data protection laws, can be criminally prosecuted in many countries and result in claims for compensation of damage. In addition, violations for which individual employees are responsible can lead to sanctions under employment law.

14.2. Data Protection Officers

Envoy Partnership has appointed a Data Protection Officers ("DPO"). The DPO is the internal and external contact for data protection. They can perform checks and must familiarise the employees with the contents of this Data Protection Policy and applicable legislation. The relevant management is required to assist the DPO with their efforts. The main tasks of the DPO are:

- To inform and advise the organisation and its employees about their obligations to comply with the applicable data protection laws and this Data Protection Policy.
- To monitor compliance with the data protection laws, including managing internal data protection activities, advise (not to conduct) on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).
- To report to the highest management level of Envoy Partnership
- To operate independently of professional orders, and is not dismissed or penalised for performing their task.
- To be provided with adequate resources to enable the DPO to meet their obligations under the applicable data protection laws and this Data Protection Policy.

15. Derogation

In exceptional cases, it may be possible to obtain a derogation from this Policy, prior to any intended processing of the Personal Data affected. Any such derogation may only be granted following a full data protection impact assessment to establish and assess the risks to any affected Data Subject, legal risks and reputational impact and is subject to approval by the directors.

16. Glossary

Data Controller/Controller/Joint Controller

This is the person or organisation which determines the purposes for and the manner in which any Personal Data is processed. It is responsible for establishing practices and policies in line with the applicable legal requirements. In most cases where Envoy is receiving sample from client, it will be joint controller of the data collected. This extends to the data we collected, even where we have assured the respondents of the confidentiality of their answers. The responsibilities and obligations of the joint controllers have to be documented and clarified in a written agreement. Some jurisdictions use other expressions for the same concept, like **Responsible Person, Organisation, Operator** etc.

Data Users

These are those of our employees whose work involves processing Personal Data. Data users must protect the data and Personal Data they handle in accordance with this Policy and any applicable data security procedures at all times.

Data processor or Processor

This is the person or organisation that is not a Data User that processes Personal Data on behalf and on instructions of the Controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle Personal Data. Envoy will variously be a Controller (e.g. in respect of our panellists or ad-hoc sample Envoy recruits for a survey) or a Processor (e.g. in respect of sample provided by clients). Some jurisdictions use other expressions for the same concept, like **Third Party, Intermediary, Operator** etc.

Data Subjects

For the purpose of this Policy include all living individuals about whom an Envoy Company hold Personal Data. A Data Subject need not be a countries national or resident. All Data Subjects have legal rights in relation to their personal information.

Personal Data

The GDPR's definition of Personal Data (GDPR Article 4 (1)) makes it clearer what Personal Data are and shows that this must be widely interpreted:

> *"…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 identity of that natural person".*

A natural person is a living individual and the GDPR itself does not apply to deceased individuals. However, individual member states may provide for rules concerning the processing of Personal Data even in respect of deceased persons.

Information about a company will not constitute Personal Data.

One has to acknowledge that it is not always possible to determine with absolute certainty, whether an individual item of information would constitute Personal Data. It will be necessary to consider the overall information held about the person in question or the means reasonably likely to be used to identify a person. With the ever improving technological means, more data will become Personal Data.

Processing

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data.

Special categories of data (p/k/a personal sensitive data)

"Special categories of Personal Data" is the new expression used in the GDPR and was previously referred to as "sensitive data". This is now defined in Article 9 GDPR as data concerning the:

"racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data [see below], biometric data [see below] for the purpose of uniquely identifying a natural person, data concerning health [see below] or data concerning a natural person's sex life or sexual orientation"

For some of these expressions more detailed definitions have been provided in the GDPR:

'genetic data' means Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

'biometric data' means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

'data concerning health' means Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Anonymous Data

This has been defined as information which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable (GDPR Recital 26). This must be distinguished from data which, together with the use of additional information (e.g. a key), could be used to identify a natural person, then the data were merely pseudonymised.

Pseudonymised data still fall under the definition of Personal Data and full GDPR principles and requirements will still apply to them.

Pseudonymisation

Pseudonymisation means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person. (GDPR Article 4(5))

Pseudonymous data refers to a data from which identifiers in a set of information are replaced with artificial identifiers, or pseudonyms, that are held separately and subject to technical safeguards. *Pseudonymised data remain Personal Data and therefore all other data protection requirements continue to apply to them!!*

PII or Personally Identifiable Information

This term derives from US privacy legislation. Although from a practical perspective applicable to Envoy's day-to-day working, the expressions Personal Data and PII can be treated as synonymous, the use of the expression PII in the context of the GDPR has to be avoided, as it otherwise negatively impacts on our

obligation to demonstrate compliance. Regulators are very keen on consistency and accuracy in the use of expressions.

PHI or Protected Health Information

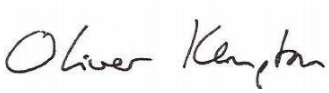
This term also derives from US privacy legislation, in particular HIPPA. Although from a practical perspective applicable to Envoy's day-to-day working the expressions special categories of Personal Data and PII should be treated as synonymous, the use of PII in the context of the GDPR should be avoided. The main issue to be considered here is that a certain Personal Data that would fall under the legal definition of PHI, under the GDPR would constitute Personal Data rather than special categories of data. For example, HIPPA would consider all information in a dataset that were to contain the name and sexual orientation as PHI, where as the GDPR would only consider the sexual orientation to be part of the special categories of Personal Data.

PSI or Personal Sensitive Information

This expression is now outdated, having derived from previous legislation. This is largely synonymous with "special categories of Personal Data" as defined in GDPR Article 9, and this expression should be used. Regulators will expect Envoy to use the correct terminology to demonstrate our compliance as part of our accountability obligation.

Policy Approval

This Policy was approved & authorised by:

Name:	Oliver Kempton
Position:	Partner
Date:	1st May 2018
Signature:	

Reviewing Policy

This policy will be reviewed and, if necessary, revised in the light of legislative or codes of practice and organisational changes. Improvements will be made to the management by learning from experience and the use of established reviews.

Policy review date: 31st January 2019

Appendix 1: Data Storage

Personal Data collected by Envoy Partnership may be stored in the following locations:

- In the Envoy Partnership offices, or on IT equipment owned by Envoy Partnership
- On Envoy Partnership cloud software. Envoy Partnership uses cloud software provided by Egnyte. Data is stored within the European Economic Area (EEA) and does not leave the EEA.
- On Envoy Partnership survey software. Envoy Partnership uses survey software provided by SurveyGizmo and by Sinzer. Data is stored within the EEA and does not leave the EEA.
- On Envoy Partnership email servers. Envoy Partnership uses Microsoft as an email provider. Data is stored within the EEA and does not leave the EEA.

Appendix 2: Responsibilities for Data Protection

As of 1st May 2018, the following named individuals hold specific responsibilities for Data Protection within Envoy Partnership

Company Partners:

- Andy Gawin Warby
- Oliver Kempton

Data Protection Officer

- Oliver Kempton

Appendix 3: Policy Implementation

Policy Implementation

To meet our responsibilities, staff will:

- Ensure any personal data is collected in a fair and lawful way
- Explain why it is needed at the start
- Ensure that only the minimum amount of information needed is collected and used
- Ensure the information used is up to date and accurate
- Review the length of time information is held
- Ensure it is kept safely
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do
- Any disclosure of personal data will be in line with our procedures
- Queries about handling personal information will be dealt with swiftly and politely

Training

Staff who have data protection responsibilities are trained annually in data privacy. Other staff are also trained on inception, and then annually.

Subject Access Requests

Anyone whose personal information we process has various rights; these are outlined in section: *8. Rights of the Data Subject*. Any person wishing to exercise this right should apply in writing to Oliver Kempton at: oliverkempton@envoypartnership.com.

We may make a charge of £10 on each occasion access is requested. We may also require proof of identity before access is granted.