Oxford Policy Management

Data Protection Policy

March 2021

Table of Definitions

In this policy the following words and phrases have the following meaning:

Definitions	
Act	means the Data Protection Act 2018.
ARCC	means the Audit, Risk and Compliance Committee.
Board	means the board of directors of OPM.
Branch Office	means any branch, representative, liaison, project office or other equivalent office in any country in which OPM operates.
Controller	means the organisation who determines the purpose and means of processing Personal Data.
Data Subject	means all natural persons (i.e. individuals) whose Personal Data is processed by OPM including, inter alia, job applicants, employees, directors, next of kin and any dependants of employees and directors, trustees, shareholders, temporary workers, consultants, fellows, agents, contractors, enumerators, respondents to OPM Surveys, interns and volunteers. The term also includes any representative (being a natural person) of any corporate client, partner, sub-contractor and supplier of OPM and also includes any other third parties who are individuals and whose data is processed by the Organisation e.g. visitors to OPM's premises, website users, OPM newsletter subscribers; survey respondents etc.
DPO	means OPM's Data Protection Officer from time to time.
EEA	means the European Economic Area.
EU	means the European Union.
GDPR	means the General Data Protection Regulation (Regulation (EU) 2016/679).
HMRC	means Her Majesty's Revenue Commissioners.
ICO	means the UK Information Commissioners Office and any successor.
International Office	Means an OPM office outside of the UK regardless of its status as a Branch Office or OPM subsidiary.
Law	means GDPR and the Act.
OPM	means Oxford Policy Management Limited, its Branch Offices and its subsidiaries as appropriate.
OPM Subsidiary	means a subsidiary of Oxford Policy Management Limited whether located in the UK or overseas and a "subsidiary" is a company in which OPM is the sole shareholder, or one of two or more shareholders in which OPM holds the majority of the voting rights or right to appoint/remove the majority of the board of directors of the company.

Personal Data	means any information relating to an identifiable natural person who can be identified, directly or indirectly, in particular, by reference to an identifier.
Policy	means this Data Protection Policy.
Processing	means any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.
Processor	means the organisation responsible for Processing Personal Data on behalf of a Controller.
Register	means OPM's record of Processing activities, which is maintained by the Organisation pursuant to its obligations under the Law respectively as a Controller and Processor of Personal Data.
Related Policies	means OPM's organisational policies, operating procedures or processes described in Section 2 of this Policy.
Special Categories of Personal Data or sensitive Personal Data	means racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. Information regarding criminal convictions and offences, though not classified as Special Category Personal Data under the Law, is treated as such by OPM and is subject to the additional safeguards required by Law.
Staff	means all employees, directors, shareholders (individuals and not entities), temporary workers, sub-contractors (individuals and not entities), interns and volunteers of the Organisation.
Subsidiary Board	means the board of directors of an OPM Subsidiary.
Supplier and Suppliers	means any person or entity delivering goods and or services to OPM.
UK	means the United Kingdom.

1. Introduction

1.1 Oxford Policy Management Limited respects the fundamental rights and freedoms of all individuals with regard to the processing of their Personal Data, whatever their nationality and residence. The organisation strives to uphold principles and rules regarding the processing of Personal Data across its worldwide operations.

1.2 OPM is fully committed to ensuring compliance with all applicable national laws about the processing of Personal Data and the privacy rights of individuals, in particular, without limitation, the UK Data Protection Act 2018, and the General Data Protection Regulation (Regulation (EU) 2016/679).

2. Purpose

2.1 This Data Protection Policy sets out how OPM seeks to:

a. comply with data protection legislation,

b. protect Personal Data; and

c. ensure that all Staff understand the rules governing their use of any Personal Data to which they have access during the course of their work.

3. Application & Scope

3.1 OPM

3.1.1 OPM recognises that the correct and lawful treatment of Personal Data maintains confidence in the Organisation and enables successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that OPM takes seriously at all times. The Organisation is exposed to potential fines (and other sanctions) for Personal Data breaches. Under the Law, a failure to comply can lead to fines as high as EUR20, 000, 000 or 4% of OPM's total worldwide annual turnover, whichever is higher and depending on the breach.

3.1.2 This Policy applies to ALL Personal Data that OPM Processes regardless of the media on which that data is stored or whether it relates to past or present Data Subjects.

3.1.3 All Staff and Suppliers must comply with this Policy. Failure to comply could lead to disciplinary action being taken against members of Staff or termination of a member of Staff's or a Supplier's relationship with OPM.

3.2 OPM Subsidiaries

3.2.1 All OPM Subsidiaries uphold the privacy standards set out in this Policy and, each Subsidiary Board

a. will adopt this Policy, subject to appropriate modification, to comply with local law; and,

b. has oversight for the effective safeguarding of Personal Data and compliance by staff with data protection policies and procedures within its company in line with group policies, procedures and practices.

3.3 Related Policies

3.3.1 This Policy is related to other organisational policies, procedures and or processes, which cover different aspects of the ways in which OPM seeks to protect the Organisation's data including its Personal Data. These policies include:

a. IT & Information Security Policy,

b. IT Acceptable Use Policy,

c. IT & Information Security Incident Response Plan,

d. Data Retention Guidelines,

e. Recruitment Policy,

f. OPM Disciplinary Policy and Procedure,

g. Cookie Policy,

h. Privacy Notice,

i. CCTV Policy; and

j. any departmental procedures, processes and guidance for the protection of Personal Data.

4. Roles and Responsibilities

4.1 The Board is ultimately responsible for ensuring that OPM, at all times, operates within the applicable statutory framework and to the highest ethical and moral standards. The Board reviews and approves this Policy every two (2) years or more frequently as circumstances demand e.g. on publication of new regulatory guidance by a regulator.

4.2 The Board has delegated its oversight responsibilities for overseeing the effectiveness of the management of OPM's data protection obligations to the ARCC. The ARCC reports to the Board quarterly or more frequently as circumstances dictate.

4.3 The SMT designs, implements and reviews the technical and organisational measures and controls to minimise the risk of Personal Data security breaches and reports to the ARCC on a quarterly basis or more frequently as circumstances dictate.

4.4 In any jurisdiction in which there is no mandatory requirement by Law to appoint a DPO, OPM elects not to make such an appointment and the Head of Legal is responsible for data protection matters in such countries. In any country in which the appointment is mandatory under national law, OPM will appoint a DPO.

4.5 The CEO and the other members of the SMT, all other staff with management accountabilities, including those responsible for Country Offices, Project Managers and other senior Staff are responsible for ensuring that all Staff within their respective offices or teams comply with this Policy (and the privacy standards contained in it). They will also develop and implement appropriate practices, processes, controls to ensure that compliance.

4.6 All Staff must be familiar with and comply with all aspects of this Policy. Staff are required to undergo mandatory data protection training and ensure that direct reports, if any, do the same. Staff are also required to regularly review any systems and processes under their control to ensure compliance with this Policy and that any governance and or operational controls are in place to ensure the proper use and protection of Personal Data.

5. OPM's Status

5.1 OPM recognises that as well as acting as a Controller of Personal Data, the Organisation may from also act as a Processor of Personal Data on behalf of another Controller, typically a donor or client. Depending on its status, OPM will have varying degrees of responsibility under the Law and in terms of liability between parties for Personal Data breaches. Occasionally, OPM may together with another organisation act as a joint Controller of Personal Data or, alternatively the parties may act as independent Controllers.

5.2 OPM's status is determined by the factual circumstances of the relationship[1]. If there is in any doubt as to OPM's status e.g. on a project, You should refer the matter to the Legal Team.

5.3 OPM and all of its Staff who handle Personal Data for OPM as part of their job-related activities will ensure that adequate safeguards are in place for the protection of that Personal Data regardless of OPM's status. This may range from practical measures such as restricting circulation of the Personal Data to small groups of people, or ensuring that CVs and other documents containing Personal Data are not left visible and unattended on worktops or computer screens; avoiding "reply all" responses on email etc through to investing in and implementing adequate organisational and technical measures to safeguard Personal Data e.g. training and appropriate technology and from the perspective of Staff.

6. What Personal Data Does OPM Process?

6.1 OPM Processes a wide range of Personal Data such as CVs, Candidate Application Forms, OPM surveys, email communications, Electronic fob keys, passports, and other IT, information and communication systems[2].

---

[1] Examples of OPM as a "Controller", "Processor" and "Joint Controller"

a. OPM (i.e. Project Administrators for OPM) book flights for project Staff via a travel agency. OPM is the Controller (and the travel agency is the Processor).

b. OPM acts as the supplier on a donor-funded project to jointly develop and operate a disaster relief centre in London. OPM is the Controller of all Personal Data belonging to OPM Staff and is the Processor of Personal Data belong to donor staff. OPM and the donor act as joint Controllers of any project specific Personal Data.

c. OPM as a supplier is carrying out a survey for and on behalf of a charitable foundation involving respondents on the foundation's mailing list. OPM is the Processor of the Personal Data of the respondents and the foundation as the owner of the mailing list, is the Controller.

[2] Examples of Types of Personal Data processed by OPM includes, inter alia:

a. Name, job title, physical addresses including email and IP address, work and personal mobile and landline telephone numbers.

b. Date of birth, town of birth etc.

c. Nationality and gender.

d. Marital status and details of any dependants.

e. Next of kin and emergency contact information.

f. National Insurance, driving licence, passport number and other numerical identifier.

g. Bank account details, payroll records and tax status information including results of HMRC employment status checks,

h. details of individuals interests in and connection to any intermediary company through which services may be supplied to OPM.

i. Salary information, annual leave entitlements, pension and benefits information.

j. Start date and, if different, the dates of continuous employment. Lifestyle and social circumstances.

k. Visual images (via CCTV, video and photographs).

l. Voice – voice/audio recordings.

m. Personal behaviour and habits.

6.2 OPM also Processes Special Category Data in particular, information concerning race or ethnicity, health information (including medical conditions, physical and mental health and sickness records etc.), religious beliefs, sexual orientation and political opinions. From time to time, OPM will Process details of criminal convictions and offences e.g. proposed new project team Staff where a project contains a safeguarding element (see OPM's Recruitment Policy for further details).

7. How Does OPM Process Personal Data?

7.1 OPM collects Personal Data:

a. directly from Data Subjects; e.g. Staff (including former Staff) during recruitment and the course of employment; visitors to OPM's premises or website; survey respondents as part of research projects undertaken on behalf of clients; or

b. indirectly from organisations such as Recruitment agencies, providers of psychometric testing, named referees, employment and other background screening service providers (for the purposes e.g. of supply chain protection, anti-terrorist financing , anti-bribery & corruption and sanctions screening providers, the Disclosure and Barring Service and equivalent services overseas, credit reference agencies, donors and other funding organisations, existing and former clients, partners, suppliers, agents, contractors and sub-contractors.

7.2 Personal Data may be shared internally or externally. In all cases only by Staff who handle Personal Data as part of their responsibilities or job-related activities[3].

7.3 Personal Data is Processed by OPM in numerous other ways in addition to sharing and collecting. This processing includes storing, transmitting , destroying or deleting Personal Data .

7.4 Regardless of the nature of Processing, OPM and all Staff handling Personal Data must do so in in compliance with the Law (any applicable local laws for the protection of Personal Data) and this Policy, procedures and any guidance issued pursuant to it.

---

n. Leaving/termination date and reasons for leaving employment or ceasing to provide services.

o. Personal references for employment purposes or the provision of services to OPM.

p. Location of employment or workplace.

q. Performance related information.

r. Disciplinary and grievance information.

s. Information regarding use by Staff and visitors of OPM's Information and Communications Systems.

The above list of Personal Data is not exhaustive and any additional or new Personal Data Processed by the Organisation will be recorded in the Organisation's Data Register.

[3] This is an example of how OPM may, through its Staff (who are responsible for carrying out the related activity), share Personal Data internally and externally:

a. Staff salary information is created by HR, this salary information relates to specified individuals and is Personal Data.

b. This Personal Data is shared by HR with Bid/Project Finance Managers for a proposed project. Bid/Project Finance Managers in turn, shares this information with Project Managers, Project/Bid Administrators and relevant Project Finance Staff.

c. Project Teams then share this Personal Data with the client e.g. DFID.

8. Processing of Personal Data (the Six Principles)

8.1 OPM will at all times, process Personal Data in accordance with the Six Principles:

1. lawfully, fairly and transparently;
2. for a specified legitimate purpose and in this respect, OPM shall not use Personal Data in a manner that is incompatible with its originally stated purpose. If OPM changes the purpose for which the Personal Data was originally processed, it shall inform the Data Subject accordingly;
3. in a manner which is adequate, relevant and not excessive i.e. the processing shall be limited to what is necessary in relation to the purposes for which it is processed;
4. using accurate information only and Personal Data shall where necessary be updated and inaccurate data, either corrected or deleted;
5. for such period of time only as is necessary for the purposes for which the Personal Data is being processed; and
6. securely, protected against unauthorised or unlawful processing and against accidental loss, destruction, damage using appropriate technical or organisational measures.

9. Compliance with the Six Principles

9.1 OPM will implement "Privacy by Design" (i.e. appropriate technical and organisational measures) in an effective manner to ensure compliance with the Law. The following measures ensure compliance by OPM with the Six Principles and where necessary suitable processes, procedures, rules and guidelines will be developed in keeping with these measures:

9.1 Register of Processing Activities and Record Keeping

OPM maintains a record of all of its processing activities as required by Law by way of a register which identifies the OPM's Processing activities at a corporate, programme and International Office level. Where a record of processing activity is specifically required by a client e.g. FCDO, the project team will maintain a separate record of all processing activities for that project.

The Register will be updated from time to time and delegated individuals within programmes, portfolios, projects and the International Offices are responsible for recording and updating these Processing activities including any changes.

9.2 Data Protection/Privacy Impact Assessments

9.2.1 Staff **must** conduct a Data protection impact assessment (DPIA) where any proposed Processing involves a high risk to the rights and freedoms of a Data Subject or any other significant economic or social disadvantage e.g. where the processing could give rise to discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal information protected by professional privilege, or unauthorised reversal of pseudonymisation.

9.2.2 In particular, a DPIA must always be undertaken where the Processing involves:

a. children or vulnerable adults;
b. introduction of new technology for business processing;
c. special category or criminal offence data on a large scale;
d. tracking individuals' online or offline location or behaviour;
e. a risk of physical harm in the event of a data security breach; or

f. a change to the nature, scope or purpose of any existing Processing.

9.2.3 DPIAs **may** be undertaken from time to time by OPM by as a matter of good practice to identify and minimise (via suitable mitigation) the data protection risks of a proposed initiative or activity.

9.2.4 A record of all completed DPIAs will be retained as part of programme, portfolio, project registers and comprise part of OPM's Register.

9.2.5 Where OPM is unable to mitigate high risks associated with the initiative or proposed Processing, and if it is appropriate to do so, OPM will consult its relevant regulators before Processing the Personal Data.

9.3 Lawful Basis of Processing

9.3.1 OPM only Processes Personal Data where it has a lawful basis for doing so which may be on one or more of the following bases:

a. **Contractual** – Processing is necessary for the performance of a contract to which the Data Subject is a party e.g. an employment contract or a sub-contract;

b. **Legal Obligation** – where OPM is under an obligation by law to Process the Personal Data e.g. disclosing Staff salary and other personal information to the tax authorities;

c. **Legitimate Interests** – OPM Processes a significant volume of Personal Data on the basis of its Legitimate Interests but does so only to the extent that these interests do not override the rights of Data Subject[4];

d. **Vital Interests** - where the Processing is necessary to protect the vital interests of the Data Subject e.g. protection of life. OPM only Processes Personal Data on this basis in connection with its duty of care or health & safety obligations and then only, in the manner permitted by Law in emergency life or death situations.

OPM does not rely on this basis to process health related Personal Data where it can do so on the basis of consent e.g. survey-related health data.

e. **Consent** – OPM relies on consent as a basis for Processing in connection with its marketing and promotional activities e.g. newsletter publication and media releases of videos and photographs. It may also Process Personal Data on the basis of consent where the Organisation is undertaking social research on behalf of clients, for example, surveying households regarding their income and expenditure pattern. There may be other circumstances where consent is used as a basis for Processing but these are limited and will be determined on a case-by-case basis.

Where OPM relies on consent as the basis for Processing Personal Data it will ensure that this consent is an informed one, freely given and is

---

[4] Examples OPM's legitimate interests:

a. Furtherance of OPM's business operations and services;

b. Pursuit or defence of claims, rights or litigation;

c. Fraud detection and prevention;

d. Accounting, auditing or reporting obligations and duties;

e. Intra-group transfers;

f. Communications, marketing and intelligence; and

g. Information and system security.

unambiguous. The Data Subject is entitled to withdraw their consent at any time.

f. **Public task** - being a private Organisation, OPM rarely Processes Personal Data on this ground, which requires that the Processing is necessary to perform a specific task in the public interest that is set out in law.

9.4 Special Category Personal Data

9.4.1 Where OPM Processes Special Category Personal Data, including any Personal Data relating to criminal convictions and offences, Staff will in conjunction with the Head of Legal determine the lawful basis for the Processing and will also identify which additional conditions for the Processing apply as required by Law.

9.4.2 Any condition identified will be as follow:

a. explicit consent;

b. for a purpose in connection with the obligations of OPM as a Controller or the Data Subject pursuant to employment law and social security;

c. vital interests of the Data Subject or other individual;

d. the Personal Data has manifestly been made public by the Data Subject;

e. the Processing is necessary for reasons of substantial public interest; or archiving purposes in the public interest, scientific or historical research or statistical purposes.

9.5 Records

9.5.1 OPM will record the bases and conditions of its Processing of Personal Data, Special Category Personal Data and information relating to criminal convictions and offences and inform Data Subjects of this in accordance with the Law.

9.6 Transparency

9.6.1 OPM will notify Data Subjects about:

a. what Personal Data is being collected at the time of Processing and if not collected directly from the Data Subject from whom or where;

b. the legal basis for the Processing by OPM;

c. how the Organisation will Process their Personal Data;

d. whether the Personal Data is being transferred outside of the current jurisdiction;

e. how the data will be protected;

f. who has access to their Personal Data;

g. how long the Personal Data will be kept by OPM; and

h. their rights in connection with this data.

Privacy notices will be given to all Data Subjects via suitable means. All Staff collecting Personal Data from Data Subjects for OPM whether directly or indirectly must provide Data Subjects with an appropriate privacy notice in accordance with this Policy.

9.7 Purpose Limitation

9.7.1 OPM only Processes Personal Data for specified, explicit and legitimate purposes. OPM will not Process Personal Data for a new purpose unless we obtain the consent of the individuals affect or have a clear basis in Law for the further Processing unless this is compatible with OPM's original purpose.

9.8 Data Minimisation

9.8.1 OPM will ensure that any Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. OPM will ensure staff do not Process Personal Data for any reason unrelated to their job duties and that they do not collect excessive data. OPM will ensure that any Personal Data collected is adequate and relevant for the intended purposes.

9.8.2 When Personal Data is no longer needed for specified purposes, it will be deleted or anonymised in accordance with OPM's record retention guidelines and other relevant procedures. Staff who handle Personal Data as part of their work, will do so in accordance with the following data limitation principles to identify what Personal Data is needed at any one stage, and therefore what can be omitted, erased or otherwise not shared:

9.8.3 Data Minimisation Principles

1. Does the individual know the data is being collected?
2. What is the plan to use this data?
3. Does the individual know why the data is being collected?
4. Is there a way of achieving this purpose without having to collect the data or any part of it?
5. Do the data need to be shared and if so with whom and can the number of recipients with whom it needs to be shared be limited?
6. How long will the data need to be held to achieve the purpose?
7. The possibility of:

a. anonymisation[5] of Personal Data.; or

b. pseudonymisation[6] of any Personal Data collected by the Organisation by way of an additional security measure if necessary

These measures shall be applied as appropriate to any OPM activity as appropriate to safeguard Personal Data.

9.9 Accuracy

9.9.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.9.2 You must ensure that the Personal Data that OPM uses and holds is accurate, complete, kept up to date and relevant to the purpose for which it is collected. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Appropriate procedures need to be implemented to ensure regularity of reviews on a basis appropriate to the function Processing the Personal Data e.g. HR may opt for a more frequent review than Project Acquisitions, for example, of records containing Personal Data. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data and ensure that a record of this Processing is entered in the relevant Register.

---

[5] **Anonymisation** is a process that irreversibly prevents identification of the individual to which it relates. Where this is achieved, the data is no longer Personal Data to which the Law applies.

[6] **Pseudonymisation** refers to the process of separation of data from direct identifiers so that any linkage to an identity is not possible without additional information that is held separately. Pseudonymisation only provides limited protection in terms of concealing the identity of Data Subjects

9.10 Security, Integrity and Confidentiality

9.10.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. Special Categories of Personal Data and criminal convictions data from loss and unauthorised access, use or disclosure will be protected with more strict measures to provide appropriate security.

9.10.2 OPM will develop, implement and maintain safeguards appropriate to OPM's size, scope and business, OPM's available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption, Anonymisation and pseudonymisation where applicable). OPM will regularly evaluate and test the effectiveness of those safeguards to ensure security of OPM's Processing of Personal Data. In particular, OPM will:

a. ensure the ongoing confidentiality, integrity, availability and resilience of its information technology systems;

b. maintain the ability to restore the availability and access to Personal Data in accordance with its incident response and /or disaster recovery procedures in a timely manner in the event of a physical or technical incident;

c. ensure periodic testing, assessment and evaluation of the effectiveness of technical measures for ensuring the security of the processing;

d. review new security technologies to determine their feasibility for OPM and test and implement where appropriate and financially viable; and

e. update existing security technologies and features on an appropriate basis and when released by the security vendor.

9.10.3 Appropriate procedures and technologies will be put in place to maintain the security of Personal Data, from the point of collection to the point of destruction. Personal Data or access to Personal Data will only be approved to third-party service providers or vendors who contractually agree to put adequate measures in place to comply with laws and policies to protect OPM's Personal Data. All third-party service provider contracts will be legally reviewed to ensure the adequacy of contractual safeguards for the protection of OPM's Personal Data.

9.10.4 OPM will ensure that its IT and Information Security Policy is complied with to and that the administrative, physical and technical safeguards that OPM implements and maintains to protect its data including Personal Data are effective. Data Security will be maintained by protecting the confidentiality, integrity and availability of Personal Data.

10. Data Subject Rights

10.1 Data Subjects have certain rights when it comes to how OPM handles their Personal Data. The extent of these rights depends on the basis of Processing and are not universal. These rights include the right to:

a. withdraw their consent to Processing at any time, where this consent is the basis of the Processing;

b. receive certain information about the Controller's Processing activities;

c. request access to their Personal Data;

d. prevent use of their Personal Data for direct marketing purposes;

e. ask to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

f. restrict Processing in specific circumstances;

g. challenge Processing which has been justified on the basis of OPM's legitimate interests or in the public interest;

h. request a copy of an agreement under which Personal Data is transferred outside of the current jurisdiction;

i. object to decisions based solely on automated processing, including profiling (ADM);

j. prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

k. be notified of a Personal Data breach which is likely to result in high risk to their rights and freedoms;

l. make a complaint to the relevant regulator as applicable;

m. in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

10.2 Appropriate training will be provided to ensure that Staff are able to recognise and respond to Data Subject requests and any such requests will be handled in accordance with the above procedures. No Personal Data will be disclosed to an outside party without proper authorisation.

11. Transfers Outside of the UK

11.1 As a global organisation, OPM transfers or makes accessible Personal Data to countries outside of the UK ("international transfers of data"). These international transfers of data include transfers to "third countries" i.e. countries in respect of which the EU has not made an "adequacy decision"[7] and are not covered by the EU-US Privacy Shield and are restricted transfers within the meaning of GDPR. With the withdrawal of the UK from the EU, international transfers of data are an in a period of regulatory uncertainty. OPM is aware of this uncertainty and is bringing in measures as required to ensure its transfers of personal data are compliant.

11.2 OPM has entered into data transfer agreements with the OPM Subsidiaries and other entities such as sub-contractors and partners located in third countries and implements such other additional safeguards to ensure the continued protection of Personal Data subject to these transfers including effective oversight of the management of this data by the same or similar measures as those deployed in the UK.

11.3 Prior to any international transfer of data by OPM e.g. as part of a donor funded project, a determination must be made as to whether the proposed transfer is a restricted transfer and if it is, that appropriate safeguards have been put in place to protect that Personal Data and ensure that the level of protection afforded by the Law is not undermined by these transfers.

11.4 If in doubt, contact Head of Legal or email dataprotection@opml.co.uk.

---

[7] Countries deemed to be adequate - Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Japan is currently being considered. Canada and the US are deemed to be "partially adequate" (for the Canada only if the personal data is covered the Canadian Personal Information Protection and Electronic Documents Act and in the case of the US, this adequacy relates only to personal data covered by the Privacy Shield – i.e. companies listed on the Privacy Shield List)

12. Direct Marketing

12.1 OPM is subject to certain rules and other privacy laws globally, such as the UK Privacy and Electronic Communications Regulations 2004 as amended when marketing potential opportunities to its consultant networks and subscribers to its newsletters. Appropriate guidance shall be published to from time to time to ensure that OPM's marketing activities do not breach these laws.

12.2 OPM will ensure that the right to object to direct marketing is explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information and will promptly honour a Data Subject's objection to direct marketing. Where a Data Subject opts out at any time, their details will be suppressed as soon as possible and in accordance with OPM's Record Retention Guidelines. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

12.3 OPM will draft guidelines on direct marketing to individual consultants/sub-contractors including representatives (who are natural persons) of any companies that OPM markets to the extent that these individuals are all Data Subjects and their Personal Data is protected by Law.

13. Personal Data Breaches

13.1 OPM shall ensure that it maintains robust breach detection, investigation and internal reporting procedures in order to facilitate OPM's decision-making about whether or not we need to notify OPM's regulators and any affected individuals of a Personal Data Breach.

13.2 A Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. This includes breaches that are the result of both accidental and deliberate causes.

13.3 Examples of Personal Data Breaches given by UK ICO:

a. access by an unauthorised third party;

b. deliberate or accidental action (or inaction) by a controller or processor;

c. sending personal data to an incorrect recipient;

d. computing devices containing personal data being lost or stolen;

e. alteration of personal data without permission; and

f. loss of availability of personal data.

13.4 A breach is often more than just about losing Personal Data and it may have information security implications. Therefore, any data breach will be dealt with in accordance with OPM's IT & Information Security Incident Response Plan which deals with the management of all information security incidents including those involving Personal Data Breaches.

13.5 Staff will be required to comply with any guidance issued pursuant to this Policy and the IT & Information Security Incident Response Plan and undergo training from time to time, to recognise information security incidents. Responsibility for the management of Personal Data implications of an incident rests primarily with Head of Legal acting in accordance with the Plan.

13.6 OPM will document and record all security incidents, even if they do not all need to be reported by Law. OPM will also keep a record of any security incidents whether or not they involve a Personal Data Breach and regardless of whether it is required to notify a client or a regulator.

13.7 The SMT and if appropriate, ARCC, must after adequate investigation, be informed of any Personal Data breach requiring notification to the relevant regulator in accordance with the IT & Information Security Policy and associated IT & Data Security Incident Response Plan.

13.8 OPM requires staff to comply with the rules prescribed by the Organisation for the notification of Personal Data breaches as set out in any policy or procedures including, without limitation, the IT & Data Security Incident Response Plan. Failure may lead to disciplinary action, and summary dismissal in serious cases.

13.9 In the event of an information security incident or concern, regardless of whether they think that this involves a Personal Data breach, Staff are required to report it by emailing: it.security@opml.co.uk rather than investigating the matter themselves.

14. Communication & Training

14.1 OPM is required to ensure all Staff have undergone adequate training to enable them to comply with data privacy laws. All Staff must therefore undergo all mandatory data privacy related training and managers must ensure their team undergo similar training. OPM maintains a record of training attendance and participation by Staff.

14.2 Guidance will be published from time to time to enable Staff to comply with this Policy and their obligations under it. OPM shall make it clear to its Suppliers that they have an obligation to provide data protection training to their staff.

14.3 A staff member's line manager or OPM Lead contact shall be the first point of contact for any data protection or privacy questions including any questions about this Policy.

14.4 Otherwise contact:

by post: Head of Legal, Oxford Policy Management Limited,
Clarendon House, Level 3,
52 Cornmarket Street, Oxford,
OX1 3HJ UK

or to any of OPM's international offices using the link provided for the address of the relevant office: https://www.opml.co.uk/contact#[insertrelevantoffice]; or

email: dataprotection@opml.co.uk.; or

telephone: Head of Legal: +44 1865 207300

Data Protection Policy

Document Purpose:

To set out our policy in regards to Data Protection

Policy Overview			
Policy Owner	Company Secretary		
Applies to	All employees and suppliers		
Global or local scope	Global		
Version Number	3.0	**Effective from**	26 March 2021
Approvals (Dates)		**Board**	26 March 2021
		Policy Authorisation Committee	11 March 2021
		Other (please state)	N/A