Privacy Notice

Updated: 26 March 2021

What is the purpose of this document?

OPM is committed to protecting the privacy and security of your personal information and this privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with data protection law.

It applies to all current and former employees, workers and contractors.

Oxford Policy Management Limited ("OPM") is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

Data protection principles

1. We will comply with data protection law. This says that the personal information we hold about you must be:
2. Used lawfully, fairly and in a transparent way.
3. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
4. Relevant to the purposes we have told you about and limited only to those purposes.
5. Accurate and kept up to date.
6. Kept only as long as necessary for the purposes we have told you about.
7. Kept securely

The kind of information we hold about you

Personal information (or personal data), means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are **special categories** of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation.

We will collect, store, and use the following categories of personal information about you:

a. Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
b. Date of birth.
c. Gender.
d. Marital status and dependants.
e. Next of kin and emergency contact information.
f. National Insurance number and other identification documents such as passport and driving licence
g. Bank account details, payroll records and tax status information.
h. Salary, annual leave, pension and benefits information.
i. Start date and, if different, the date of your continuous employment.
j. Leaving date and your reason for leaving.
k. Location of employment or workplace.
l. Copy of driving licence.
m. Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
n. Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
o. Compensation history.
p. Performance information.
q. Disciplinary and grievance information.
r. CCTV footage and other information obtained through electronic means such as swipe card records.
s. Information about your use of our information and communications systems.
t. Photographs.
u. Results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied.

We may also collect, store and use the following **special categories** of more sensitive personal information:

a. Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
b. Trade union membership.
c. Information about your health, including any medical condition, health and sickness records, including:
d. where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
    i. details of any absences (other than holidays) from work including time on statutory parental leave and sick leave;

ii. where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes; and
iii. Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, named referees, credit reference agencies, providers of psychometric testing, Disclosure and Barring Service or other background check agencies.

As part of our Due Diligence process we screen all employees using publicly available datasets including national and international watch lists and media archives. We do this in order to meet client requirements and to protect vulnerable people with whom our staff may come into contact as well as to identify serious issues such as suspected terrorism or money laundering. While you remain an employee of OPM there will be an automatic search against your name so that any possible issues will be flagged. In the unlikely event that we identify a potential issue, we will discuss this with you.

We will also check to see if you are on the register of 'Politically Exposed Persons' or have a close link to someone who is. This is to ensure that you are not put in a position where you may potentially have a conflict of interest or your neutrality could be questioned.

We will collect additional personal information in the course of job-related activities throughout the period that you work for us.

How we will use personal information

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our **legitimate interests** (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

Legitimate Interests

Legitimate interests include, but are not limited to:

a. to carry out OPM's business operations, services and products

b. to carry out our HR and Marketing functions and initiatives

c. the pursuit or defence of any claims, rights or litigation or detection of a crime

d. our accounting or auditing functions and reporting duties

e. to support OPM's commercial development, strategy, planning or growth including any business sales or transactions

f. the protection of the OPM's intellectual property rights, confidential information, security or product development

g. monitoring and ensuring compliance with our policies, processes and procedures such as security, fraud prevention, employee benefits and training

h. general security purposes and to fulfil our duty of care obligations

Situations in which we will use your personal information

We need all the categories of information listed above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

The situations in which we will process your personal information are listed below.

a. Making a decision about your recruitment or appointment.

b. Determining the terms on which you work for us.

c. Checking you are legally entitled to work in the UK.

d. Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).

e. Providing benefits to you.

f. Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.

g. Liaising with the trustees or managers of a pension arrangement operated by a group company, your pension provider and any other provider of employee benefits.

h. Administering the contract we have entered into with you.

i. Business management and planning, including accounting and auditing.

j. To complete costing information for Invitation to Tender documents, which in certain circumstances may include providing and disclosing salary information.

k. Conducting performance reviews, managing performance and determining performance requirements.

l. Making decisions about salary reviews and compensation.

m. Assessing qualifications for a particular job or task, including decisions about promotions.

n. Gathering evidence for possible grievance or disciplinary hearings.

o. Making decisions about your continued employment or engagement.

p. Making arrangements for the termination of our working relationship.

q. Education, training and development requirements.

r. Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.

s. Ascertaining your fitness to work.

t. Managing sickness absence.

u. Complying with health and safety obligations

v. To ensure your security when working oversees and to fulfil our duty of care obligations.

w. To prevent fraud, breaches on intellectual property rights, unauthorised access to our IT systems or to detect a crime.

x. To monitor your use of our information and communication systems to ensure compliance with our IT policies.

y. To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

z. To conduct data analytics studies to review and better understand employee retention and attrition rates.

aa. Equal opportunities monitoring.

bb. Business sales or acquisitions including due diligence processes.

cc. Providing references (including reference to mortgage companies).

dd. Registering the status of protected employees.

ee. Accessing data from third parties if from a publicly accessible source (e.g. Facebook or other social media sites).

Some of the grounds relied on for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers). In certain circumstances, failure to provide information could be a disciplinary issue and could lead to termination of your employment or engagement with OPM.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use Special Categories of personal information

Special categories of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

a. We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.

b. We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance.

c. If you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, we will use information about your physical or mental health, or disability status in reaching a decision about your entitlements under the share plan.

d. If you apply for an ill-health pension under a pension arrangement operated by a group company, we will use information about your physical or mental health in reaching a decision about your entitlement.

e. We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

f. We will use information to register the status of a protected employee which you are required to provide to us and to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We envisage that we will hold information about criminal convictions.

We can only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Privacy Standard.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Where appropriate, we will collect information about unspent criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in order to decide whether an employment candidate's criminal history poses a risk for OPM in the context of the role the individual is applying for.

We are allowed to use your personal information in this way to carry out our obligations under the contracts we have with funding organisations and clients. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We may share your data with other legal entities in the OPM group in order that we can carry out our duties under our contract with you or to enable us to carry on our legitimate business.

We may need to share your data with third parties, which may include clients or third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with applicable laws and regulations.

We may transfer your personal information outside of the UK or the EEA. If we do, you can expect a similar degree of protection in respect of your personal information in the way we process it unless we have notified you in advance of whom we are sharing the data with.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. For example, the following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services and security services.

We will share personal data regarding your participation in any pension arrangement operated by a group company with the trustees or scheme managers of the arrangement in connection with the administration of the arrangements.

The recipients or categories of recipients of the Data may include the following:

a. Parent or Group Companies

b. Legal representatives

c. Accountants

d. Auditors

e. Recruiters or reference checking agencies
f. Pensions or other insurance providers (including brokers)
g. Government or statutory bodies
h. Non-government bodies
i. HMRC, regulators, professional bodies and other authorities
j. Insurers, insurance brokers
k. Occupational health providers
l. Medical practitioners, clinicians, doctors, other health providers and consultants
m. Payroll providers
n. Marketing or PR agencies
o. Service providers who provide IT and system administration services and cloud service providers who host our systems
p. Clients or customers (for the purposes of assessing suitability for a project or specific piece of work)
q. Training providers and providers of testing services
r. Industry regulators
s. DVLA
t. Disclosure and Barring Service
u. Consultants or Contractors working on our behalf
v. Enquiry agents or investigators
w. Providers of security services

This list may include an employer or third party recipient(s) outside of the UK or the European Economic Area (EEA). This list is non-exhaustive.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our activities to carry out the contracts gain further contracts.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC and disclosures to shareholders such as directors' remuneration reporting requirements.

International Transfers

We share your personal information within the OPM Group. This will involve transferring your information to the UK if this is outside of your employing offices jurisdiction and it may also be transferred outside of the UK and the European Economic Area (EEA). Some of the external third party service providers that we engage as processors are also based outside of the UK or the EEA. Where we share your personal information with such providers or within the OPM Group, we will ensure a similar degree of protection is afforded to it and will abide by data protection laws with regard to such a transfer and ensure that there are appropriate safeguards in place or that the transfer is to a country deemed by the European Commission to provide an adequate level of protection for personal information subject to the below.

Where you work with us on a project based outside of the your employing jurisdiction, the UK or the EEA, your personal information may be provided to our staff, consultants, suppliers, clients and other organisations working with us on the project and who are located in countries where standards of data protection are not as stringent as those that apply within the UK or the EEA. Such transfer is necessary in the performance of your role with OPM and may also be necessary in order to comply with our legal obligations and to protect your interests (for example where we transfer your personal information for security reasons to protect your well-being).

Data security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained by contacting data.protection@opml.co.uk.

Data retention

We will only keep your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our Privacy Standard and applicable data protection laws and regulations.

Further details and examples are set out in the Privacy Standard.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Rights of access, correction, erasure, and restriction

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

1. **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

2. **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

3. **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

4. **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

5. **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

6. **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact data.protection@opml.co.uk in writing.

Fees

You will not have to pay a fee to access your personal information (or to exercise any of the other rights).

But, if your request for access is clearly unfounded or excessive we may charge a reasonable fee or alternatively, we may refuse to comply with the request.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact data.protection@opml.co.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. Your withdrawal will not affect any processing that we have done previously on the basis of your consent.

Data Privacy Manager

We have appointed a data privacy manager to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the data privacy manager, using the email address ‘dataprotection@opml.co.uk’. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact mailto:data.protection@opml.co.uk.