

Privacy policy for Frazer-Nash's UK employees and workers

WHO WE ARE

Frazer-Nash Consultancy Limited (company number 02562870, whose registered office is at: Hill Park Court, Springfield Drive, Leatherhead, Surrey, England, KT22 7NL) (“Frazer-Nash”, “we”, “us”, “our”) collects, uses and is responsible for certain personal data about you. When we do so, we are subject to the Data Protection Act 2018, and the UK General Data Protection Regulation, any national implementing laws, regulations and secondary legislation, and any related or successor legislation on data protection (“**Data Protection Law**”)

WHAT IS THE PURPOSE OF THIS POLICY?

This Policy describes how we collect and use personal data about you during and after your working relationship with us.

This Policy applies to current and former employees, workers and third-party contractors “**Associates**”. The Policy also covers individuals who are engaged by us on a temporary basis such as temporary staff, secondees, student placements and work experience.

Please read this Policy carefully, together with any other policy or notice relating to your personal data which we may provide on specific occasions when we are collecting or processing personal data about you.

TERMINOLOGY USED IN THIS POLICY

When we refer to “**personal data**” in this Policy, we mean any information about an individual which can be used to identify that individual.

When we refer to “**special category personal data**” in this Policy, we mean types of personal data which require a higher level of protection, for example, information revealing racial or ethnic origin, political opinions or religious beliefs.

For the purposes of Data Protection Law, we are a “**data controller**”. This means that we are responsible for deciding how we hold and use personal data about you.

When we refer to “**corporate group**” we mean Frazer-Nash Consultancy, its business units, affiliates, subsidiaries, and successors. “**Affiliates**” under this definition of corporate group shall include Kellogg Brown & Root Limited and its affiliates, subsidiaries, and successors.

PERSONAL DATA WE COLLECT ABOUT YOU

We may collect, store, and use the following categories of **personal data** about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Business contact details such as name, title, addresses, telephone numbers and business email addresses
- Date of birth
- Gender
- Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Start date and, if different, the date of your continuous employment or engagement
- Leaving date and your reason for leaving
- Details of the office at which you are based
- Copy of driving licence
- Copy of identification information (for example passport, birth certificate, utility bill)
- 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).

Privacy policy for Frazer-Nash's UK employees and workers

- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Compensation history
- Payroll data
- Performance information
- Disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as swipe card records
- Information about your use of our information and communications systems
- Photographs
- Fees, charges and other payment information
- Details of previous engagements
- Details of engagements with Frazer-Nash

We may also collect, store and use the following **special category personal data**:

- Information about your race or ethnicity, nationality, religious beliefs, sexual orientation and political opinions
- Information about your health, including any medical condition, disability, health and sickness records, including:
 - where you leave employment or engagement due to ill-health, injury or disability, the records relating to that decision
 - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave
 - where you leave employment or engagement and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.

We may also collect, store and use personal data relating to **criminal convictions and offences**. Please see below for further information about our collection and use of such information.

HOW IS YOUR PERSONAL DATA COLLECTED?

We collect personal data about employees and workers through the application and recruitment/on-boarding process, either directly from the individual or sometimes from an employment agency or background check provider.

We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We may also collect additional personal data in the course of job-related activities throughout the period of you working for us.

HOW WE USE INFORMATION ABOUT YOU

Under Data Protection Law, we can only use your personal data if we have a proper reason and legal basis for doing so. Most commonly, we will only use your personal data in the following circumstances:

- (i) in order to perform the contract we have entered into with you (for example, your employment contract or services agreement); or
- (ii) where we need such personal data in order to comply with a legal obligation; or
- (iii) 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.

Situations in which we will use your personal data

Some situations in which we may process your personal data are listed below.

- Where we are required by a customer, potential customer or other corporate group company to include details of your CV, working history or similar in connection with a bid or a project

Privacy policy for Frazer-Nash's UK employees and workers

- Making a decision about your recruitment or engagement
- Determining the terms on which you work for us
- Checking you are legally entitled to work in the UK
- Paying you and, where applicable, deducting tax and National Insurance contributions (NICs)
- Providing any benefits to you which we have agreed to provide in your employment or services contract
- Enrolling you in the company our pension scheme if applicable
- 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
- Administering the contract we have entered into with you
- Business management and planning
- Conducting appraisals, managing performance and determining performance requirements
- Making decisions about salary reviews, compensation
- Assessing qualifications and expertise for a particular project or task, including decisions about promotions
- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Education, training and professional development requirements
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
- Ascertaining your fitness to work
- Complying with health and safety obligations
- Preventing fraud
- Monitoring your use of our information and communication systems to ensure compliance with our IT policies
- Ensuring network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- Conducting data analytics studies to review and better understand employee retention and attrition rates
- To obtain security clearance and/or permit you to work on certain client projects

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

If you fail to provide personal data

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).

Change of purpose

We will only use your personal data 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 data 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 data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE “SPECIAL CATEGORY” PERSONAL DATA

Where it is necessary for us to collect special category personal data (as defined above), we will ensure that such information is suitably protected. We may process special categories of personal data in the following circumstances:

- (i) in limited circumstances, with your explicit written consent; or

Privacy policy for Frazer-Nash's UK employees and workers

- (ii) where we need to carry out our legal obligations or exercise rights in connection with employment and engagements; or
- (iii) where it is needed in the public interest, such as for equal opportunities monitoring; or
- (iv) less commonly, we may process this type of information where it is needed in relation to legal claims.

Situations in which we will use your “special category” personal data

Some situations in which we may process your “special category” personal data are listed below:

- 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.
- 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 health insurance all in accordance with current legislation.
- We may 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 and to comply with our obligations under the Equalities Act 2010.
- We may need to obtain and process information about your nationality and other personal data for reasons of national security in order to obtain security clearance and/or permit you to work on certain client projects. Processing personal data for national security reasons is exempt from some aspects of Data Protection Law.

INFORMATION ABOUT CRIMINAL CONVICTIONS

Owing to Frazer-Nash's involvement in work pertaining to national security, we are required by the Cabinet Office's "Baseline Personnel Security Standard" to carry out criminal record checks using the Disclosure and Barring Service ("DBS") (or "Disclosure Scotland" in Scotland).

This is a legal requirement for us under the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended).

Whilst it is true that not all our employees and workers will be involved in work relating to national security, the fact that Frazer-Nash operates an open office environment means that employees and workers could find themselves working alongside individuals that are, and on this basis, we have taken the view that we have a legitimate business interest in carrying out criminal record checks for *all* employees and workers.

We only hold such information for such time as is necessary in order to complete the required checks, thereafter, we will take steps to ensure secure destruction of the information.

WHO WE SHARE YOUR PERSONAL DATA WITH

There may be circumstances where we share your personal data with third parties. In such circumstances, we will adhere to Data Protection Law.

These "third parties" may include other entities within our corporate group, potential customers or, regulatory bodies. It may also include service providers who perform tasks for us such as security clearance checks, payroll, insurance services, banking services, pension administration, benefits provision and administration and IT service providers (such as printing or website hosting).

Less commonly, we may also need to share some personal data with other parties, such a potential buyer of some or all of our business or during a re-structuring. Usually, in such circumstances, the information will be anonymised, but this may not always be possible. In any case, we will ensure that any such recipients are bound by confidentiality obligations.

We will only disclose your personal data to such third parties in the following circumstances:

- (i) where we are required by law to do so (for example, making returns to HMRC)

Privacy policy for Frazer-Nash's UK employees and workers

- (ii) where it is necessary to administer the working relationship with you
- (iii) we have another legitimate interest in disclosing the information to such third parties.

We require third parties to respect the security of your data and to treat it in accordance with the law. In many scenarios, such third parties are likely to be “data processors” for the purposes of Data Protection Law. In any case, we require all third parties to respect the security of your data and to treat it in accordance with the law.

KEEPING YOUR PERSONAL DATA SECURE

We have appropriate security measures in place to prevent your personal data from being accidentally lost, or used or accessed unlawfully. We limit access to your personal data to those who have a genuine business need to know it. Those processing your personal data will only do so in an authorised manner and are subject to a duty of confidentiality.

In the event that we become aware of an actual or suspected data security breach, we will promptly take all necessary steps to address such breach.

HOW LONG YOUR PERSONAL DATA WILL BE KEPT

We will only retain your personal data 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 data 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 or worker of the company we will retain and securely destroy your personal data in accordance with our data retention policy.

TRANSFERRING PERSONAL DATA OUTSIDE OF THE UK

As well as our network of offices in the UK, we also have several offices in Australia. As a result, it is possible that from time to time, we may transfer your personal data to Australia. This would be most likely to occur in the event that you are working with or at one of our Australian offices.

Aside from transfers to Australia, it may also be necessary from time to time, for us to transfer your personal data to other countries outside the European Economic Area (EEA) and UK. For example, where you will be working on a project outside of the EEA and UK, or where your personal data is transferred to a member of our global corporate group based in another country such as the United States of America or where your personal data is stored in databases that are accessible in other countries.

Protecting your personal data

We are aware that transfers of personal data outside of the EEA and UK are subject to special rules under Data Protection Law and will ensure that your personal data is suitably protected.

With regard to transfers of personal data to Australia, we will ensure your personal data is protected by requiring our Australian offices to comply with the EU’s model clauses on transfers of personal data outside the EEA and UK, or successor UK International Data Transfer Agreement (IDTA) clauses published by the Information Commissioner’s Office.

For transfers outside of the UK and to non-EEA countries other than Australia, we will safeguard your personal data by (i) ensuring that the transferee country is one which has been granted an EU “adequacy decision” or subsequent UK equivalent; or (ii) putting in place sufficient safeguards, in accordance with the applicable Data Protection Law, to protect your personal data. These safeguards may include putting in place data transfer agreements containing the EU model clauses (or successor UK IDTA clauses) with the party receiving the personal data.

Privacy policy for Frazer-Nash's UK employees and workers

If you would like further information, please do not hesitate to contact us.

YOUR RIGHTS AND RESPONSIBILITIES

Your duty to inform us of changes

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

Your rights in connection with personal data

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

- **Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data 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 data where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal data 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 data for direct marketing purposes.
- **Request the restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal data to another party.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact us using the following email address datamanagement@fnc.co.uk.

For more information about your rights, you may wish to look at the Information Commissioners Office website www.ico.org.uk.

No fee usually required

You will not normally have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

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 data 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 data 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 us. 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.

Privacy policy for Frazer-Nash's UK employees and workers



HOW TO CONTACT US

If you have any questions about this Policy or how we handle your personal data, please contact the People Director using the following email address: datamanagement@fnc.co.uk.

In the event you have a complaint relating to our handling of your personal data, you also have the right to lodge a complaint with the UK Information Commissioner.

CHANGES TO THIS POLICY

We reserve the right to update this Policy at any time, and we will republish it when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data