

Introduction

Nuvia UK is committed to being transparent about how it:

- handles your personal information;
- protects the privacy and security of your personal information; and
- meets its data protection obligations under relevant legislation.

The purpose of this Privacy Notice is to make you aware of how and why we will collect and use your personal information which may be held by us on paper or in electronic format.

This Privacy Notice is non-contractual and does not form part of any employment contract, consultancy agreement or any other contract for services.

If you have any questions about this Privacy Notice or about how we handle your personal information, you can email us at info.uk@nuvia.com or write to Steve Dowell, Data Protection Officer, Nuvia UK, Chadwick House, Risley, Warrington WA3 6AE.

Your rights

Under current data protection legislation, you have rights as an individual which you can exercise in relation to the information we hold about you. You have the right to request from Nuvia UK access to and rectification or erasure of your personal data, or restriction of processing concerning you, or to object to processing, as well as the right to data portability.

Complaints or queries

Nuvia tries to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

This Privacy Notice was drafted with brevity and clarity in mind. It does not provide exhaustive detail of all aspects of Nuvia's collection and use of personal information. However, we are happy to provide any additional information or explanation needed. Any requests for this should be sent to the address below.

You have the right to lodge a complaint about the treatment of your personal data. These can be addressed to Nuvia's Data Protection Officer, Steve Dowell at the address above.

If you still are not happy you have the right to complain to the Information Commissioner's Office. Details are on their website: <https://ico.org.uk/>.

Access to personal information

Nuvia tries to be as open as it can be in terms of giving people access to their personal information. Individuals can find out if we hold any personal information by making a 'subject access request'. If we do hold information about you we will:

- give you a description of it;
- tell you why we are holding it;
- tell you who it could be disclosed to; and
- let you have a copy of the information in an intelligible form.

To make a request to Nuvia for any personal information we may hold, you need to put the request in writing to the address provided below. If you agree, we will try to deal with your request informally, for example by providing you with the specific information you need over the telephone. If we do hold information about you, you can ask us to correct any mistakes.

Changes to this Privacy Notice

We keep our Privacy Notice under regular review. This Privacy Notice was updated in February 2021.

How to contact us

If you want to request information about our privacy policy you can email us at info.uk@nuvia.com or write to: The Data Protection Officer, Nuvia UK, Chadwick House, Birchwood Park, Risley, Warrington, Cheshire, WA3 6AE.

How we use your information

This Privacy Notice tells you what to expect when Nuvia UK collects personal information. It applies to information we collect about:

1. job applicants;
2. individuals requiring security checks;
3. our current and former employees;
4. agency staff;
5. consultants;
6. radiation workers for whom we provide an Approved Dosimetry Service;
7. people who attend our radiation safety courses;
8. business contacts;
9. visitors to our websites;
10. people who use our services, e.g. who subscribe to our newsletter or request a publication from us;

1. Job applicants

What will we do with the information you provide to us?

All of the information you provide during the process will only be used for the purpose of progressing your application, or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information you provide during the recruitment process with any third parties for marketing purposes or store any of your information outside of the European Economic Area. The information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format.

We will use the contact details you provide to us to contact you to progress your application. We will use the other information you provide to assess your suitability for the role you have applied for.

What information do we ask for, and why?

We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary.

The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for but it might affect your application if you don't.

Application stage

We ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for. Our recruitment team will have access to all of this information.

You will also be asked to provide equal opportunities information. This is not mandatory information – if you don't provide it, it will not affect your application. This information will not be made available to any staff outside of our recruitment team, including hiring managers, in a way which can identify you. Any information you do provide, will be used only to produce and monitor equal opportunities statistics.

Shortlisting

Our hiring managers shortlist applications for interview. They will not be provided with your equal opportunities information if you have provided it.

Assessments

We might ask you to participate in assessment days; complete tests or occupational personality profile questionnaires; and/or to attend an interview – or a combination of these. Information will be generated by you and by us. For example, you might complete a written test or we might take interview notes. This information is held by Nuvia.

Before you start

If we make a conditional offer to you, we will ask for certain information so that we can carry out security checks before you start – see below for details of this process.

For employees, we will also ask you to complete a questionnaire about your health. This is to establish your fitness to work and whether any adjustments should be considered with regards your performance in that role in accordance with The Equality Act 2010.

You will be required to provide proof of your qualifications – you will be asked to attend our office with original documents, and we will take and retain copies.

You must successfully complete these checks to progress to a final offer.

Who do we share the information with?

We use third party recruitment agencies who provide elements of our recruitment service for us. We have contracts in place with our recruitment agencies. This means that they cannot do anything with the personal information you provide to us unless we have instructed them to do it. They will not share this information with any organisation apart from us. They will hold it securely and retain it for the period we instruct. If you contact us directly, we may ask your permission to provide your details to one of our recruitment agencies.

How long is the information retained for?

If you are unsuccessful following assessment for the position you have applied for, we may ask if you would like your details to be retained for a period of twelve months. If you say yes, we would proactively contact you should any further suitable vacancies arise.

2. Individuals requiring security checks

We are required to carry out security checks for all our employees; for anyone that we engage as hired staff through an agency or as a consultant; for anyone else who requires unescorted access to Nuvia buildings and facilities or to certain sites and facilities operated by our clients, or access to certain classes of information; and for anyone else requiring a user account on a Nuvia IT system.

These checks involve confirming your identity, your right to work in the United Kingdom and seeking assurance as to your trustworthiness, integrity and reliability, in accordance with the UK government's Baseline Personnel Security Standard (BPSS) guidance.

You will therefore be required to provide proof of your identity and your right to work in the UK – you will be asked to attend our office with original documents, and we will take and retain copies.

For jobs based in England and Wales, we will provide your email address to uCheck who will contact you to complete an application for a Basic Disclosure check via the Disclosure and Barring Service. For jobs in Scotland, we will ask you to complete an application form to obtain a Basic Disclosure check from Disclosure Scotland. If you have lived or worked outside the UK, we may ask you to obtain a police certificate from the country you lived or worked in. In all cases, the purpose of this is to verify any unspent criminal convictions that you might have.

We will also collect personal information from other external third parties, such as references from former employers, using the details you provide in your application.

Some roles require a higher level of security clearance. If this is the case, then you will be asked to submit information via the National Security Vetting (NSV) process to UK Security Vetting (UKSV) and/or the Office for Nuclear Regulation (ONR). UKSV/ONR will be the data controller for this information.

UKSV/ONR will tell us whether your application is successful or not. If it is unsuccessful, Nuvia will not be told the reason(s) why but we might need to review your suitability for the role or how you perform your duties.

We may also submit your full name and date of birth to UKSV to check whether you have an existing National Security Vetting clearance, using UKSV's Vetting Status Information (VSI) enquiry process.

As part of an annual review of BPSS and NSV clearances, we ask managers to confirm whether their staff have shown any evidence of any behaviours, conduct or illness which might cast doubt on their continued suitability for security clearance, and any issues identified may be shared with UKSV or ONR.

For access to Nuvia buildings, we will take a photograph of you for your building pass. We also ask you if you would wish to include details on the back of your building pass of your blood group and any other information that might be of benefit to medical or first aid staff in the event of an emergency; this information is not mandatory.

We also hold information on any occasions when you have used an access control system in a Nuvia building by means of a Nuvia-issued access control fob.

Who do we share the information with?

Information relevant to your security clearance may be shared with UKSV or ONR. In addition, we may provide details of your security clearance, including full name, date of birth, national insurance number and nationality, to other organisations to enable you to obtain access to sites or information which requires a specific security clearance.

How long is the information retained for?

Copies of Basic Disclosure certificate or overseas Police Certificates are retained for 12 months after your security clearance is granted, after which they are destroyed. No information relating to any criminal records is retained beyond that point.

Details relating to your security clearance are retained for 12 months after you have left Nuvia or after the reason for you holding a security clearance has ended. For former employees, copies of documentation demonstrating your right to work in the UK are retained for 2 years after you leave employment.

Building passes are destroyed when they are returned because they are no longer required.

3. Current and former Nuvia employees

What information do we ask for, and why?

During the course of your employment and beyond, we collect, use and process personal information about you. This information may include, but is not limited to:

- your emergency contact details/next of kin/dependants;
- your date of birth;
- the “Protected Characteristics” information required for compliance with the Equality Act 2010 (i.e. age, gender reassignment, being married or in a civil partnership, pregnancy/maternity leave, disability, race (including colour, nationality, ethnic or national origin), religion or belief, sex and sexual orientation);
- your marital status and dependants;
- the start and end dates of your employment;
- the terms and conditions of your employment including salary and benefits, as set out in a job offer letter, employment contract and written statement of employment particulars, pay review and bonus letters, statements of changes to employment and other related correspondence;
- details of your skills, qualifications, experience and work history, both with previous employers and with Nuvia UK;
- copies of qualification certificates;
- your National Insurance number;
- your bank account details, records, tax code and tax status information;
- any disciplinary, grievance and capability records, including investigation reports, collated evidence, minutes of hearings and appeal hearings, warning letters, performance improvement plans and related correspondence;
- performance assessments, either as part of our Personal Development Review (PDR) process or as probationary reviews, including feedback and ratings, targets and objectives set;
- annual leave and other leave records, including details of the types of and reasons for leave being taken and related correspondence;
- any termination of employment or engagement documentation, including resignation letters, dismissal letters, redundancy letters, notes of meetings, settlement agreements and related correspondence;
- information about your use of our IT systems, including telephones, e-mail and the internet;
- photographs;
- pension scheme details;
- details of sickness absence including medical reasons for absence;
- records of any training that you attend, which, together with your experience and qualifications, may be used as a business CV in support of bids for work with our customers;
- time bookings in our Agresso financial system;
- driver mandate details for employees authorised to drive for work, including a copy of your driving licence;
- relevant details for various arrangements that we operate as employment benefits for some employees, i.e. healthcare, income protection and death in service insurance, our share option scheme, and our childcare scheme;
- details of safety, health, environment, security, quality or issues raised by you or relating to you in one of our internal reporting systems – Unusual Occurrence Reports (UNORs) or Quality Observation Reports (QORs).

What is the legal basis for processing of personal data?

We will only use your personal information when the law allows us to. These are known as the legal bases for processing. We will use your personal information in the following circumstances:

- where we need to do so to perform the employment contract, consultancy agreement or contract for services we have entered into with you;
- where we need to comply with a legal obligation (e.g. gender pay gap reporting or similar);
- where it is necessary for our legitimate interests (or those of a third party), and your interests or your fundamental rights and freedoms do not override our interests.

- In more detail, we process personal data in order to:
- enable us to maintain accurate and up-to-date employee, worker and contractor records and contact details (including details of whom to contact in the event of an emergency)
- comply with the duty to make reasonable adjustments for disabled employees and workers and with other disability discrimination obligations
- maintain an accurate record of your employment or engagement terms
- administer the contract we have entered into with you
- ensure you are paid correctly and receive the correct benefits and pension entitlements, including liaising with any external benefits or pension providers or insurers
- ensure compliance with income tax requirements, e.g. deducting income tax and National Insurance contributions where applicable
- plan for career development and succession
- manage, plan and organise work
- enable effective workforce management
- operate and maintain a record of annual leave procedures
- operate and maintain a record of sickness absence procedures
- ascertain your fitness to work
- operate and maintain a record of maternity leave, paternity leave, adoption leave, shared parental leave, parental leave and any other type of paid or unpaid leave or time off work
- ensure payment of SSP or contractual sick pay
- ensure payment of other statutory or contractual pay entitlements, e.g. SMP, SPP, SAP and ShPP
- meet our obligations under health and safety laws
- make decisions about continued employment or engagement
- operate and maintain a record of dismissal procedures
- provide references on request for current or former employees, workers or contractors
- prevent fraud
- ensure compliance with our IT-related policies in your use of our IT systems
- ensure network/information security and prevent unauthorised access/modifications to systems
- ensure effective HR and business administration, including accounting and auditing
- ensure adherence to Company rules, policies and procedures
- enable us to establish, exercise or defend possible legal claims
- provide and administer benefits to our employees

Please note that we may process your personal information without your consent, where this is required or permitted by law.

Who do we share the information with?

Your personal information may be shared internally within Nuvia UK, including with members of the HR department, your line manager and other managers in your department, if access to your personal information is necessary for the performance of their roles.

Externally, we may share personal information with third parties in the context of a tendering or TUPE exercise that involves some or all of our business. In those circumstances, any personal information will be subject to confidentiality undertakings. It is typical in these circumstances that the information is collated and only presented, if it is at all, as part of a collective data submission so no one individual's data is revealed at all, or, if it has to be, it is pseudonymised.

We may also need to share your personal information with a regulator or to otherwise comply with the law, or with third parties where it is necessary to administer the contract we have entered into with you, where we need to comply with a legal obligation, or where it is necessary for our legitimate interests (or those of a third party). Third-party service providers (and their designated agents), include:

- Practical Payroll Solutions (PPS) - If you are employed by Nuvia UK, relevant personal details about you will be provided to PPS who provide payroll services to Nuvia UK. This will include your name, bank details, address, date of birth, National Insurance Number and salary to administer payroll to all employees.

- Benefits administrators, including insurers (Towergate, Mediacash, BUPA, AXA PPP, Equiniti, Zurich Assurance). We will provide any benefits administrators with relevant personal details to fulfil their duties of administering their schemes.
- Pension scheme administrators (Buck Consultants, Scottish Widows, Legal & General, Smart Pensions, Vinci). If you are a member of the Nuvia UK Employees Pension Scheme your details will be provided the Trustees of the Scheme, who will share that information with Buck Consultants and Scottish Widows who are the administrators of the Scheme, and with Vinci plc who provide administrative support to the Scheme. If you are contractually enrolled or auto-enrolled into the Nuvia Pension Plan (part of the Legal & General Master Trust) your details will be provided the Trustees of the Master Trust, who will share that information with Legal & General who are the administrators of the Scheme. If you are enrolled into the NAECI Pension Scheme your details will be provided to Smart Pensions who are the administrators of that scheme. Details provided will include your name, date of birth, National Insurance number and salary. The Trustees of these schemes may also share these details with other third parties, such as actuarial advisers, auditors, legal advisers.
- AVC scheme provider and AVC administration (Standard Group Life) – for processing transactions as part of the Additional Voluntary Contribution schemes.
- Occupational health providers (Duradiamond and DSRL). If we make you a conditional offer of employment, we will ask that you complete a questionnaire which will help to determine if you are fit to undertake the work that you have been offered, or will advise us if any adjustments are needed to the work environment or systems so that you may work effectively. There will be times when Nuvia UK will need to make a referral to Occupational Health for further support and advice on reasonable adjustments.
- SFITUK, who provide IT services to Nuvia UK.
- External auditors from clients for whom Nuvia UK work on projects as contractors to ensure compliance to contract, and other necessary audits such as LRQA.
- Professional advisers, such as lawyers and accountants (Eversheds, Analysis Legal & Mazars) for employees who are seconded, and other ad hoc advice on payroll and employment advice.
- Vinci Fleet, who provide vehicle management services to Nuvia, including management of company cars.

How long is the information retained for?

Once you have left employment or your engagement has been terminated, we will generally hold your personal information for six years (5 years in Scotland) after the termination of your employment or engagement. This is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal information to protect against legal risk, e.g. if the information could be relevant to a possible legal claim in a tribunal, County Court or High Court. We will hold payroll, wage and tax records (including salary, bonuses, overtime, expenses, benefits and pension information, National Insurance number, PAYE records, tax code and tax status information). Overall, this means that we will “thin” the file of personal information that we hold on you one year after the termination of your employment or engagement, so that we only continue to retain for a longer period what is strictly necessary.

Disciplinary, grievance and capability records will only be retained until the expiry of any warning given (but a summary disciplinary, grievance or performance management record will still be maintained for the duration of your employment).

Personal information which is no longer to be retained will be securely and effectively destroyed or permanently erased from our IS systems and we will also require third parties to destroy or erase such personal information where applicable.

4. Agency staff and consultants

What information do we ask for, and why?

Individuals that we engage through an employment agency or through a consultancy agreement are subject to the job applicant and security checking processes described in Sections 1 and 2 above, as well as some of the processes and procedures described in Section 3, namely:

- Partner and emergency contact details – so we know who to contact in case you have an emergency at work
- details of pay rates;
- records of any training that you attend, which, together with your experience and qualifications, may be used as a business CV in support of bids for work with our customers;
- time bookings in our Agresso financial system;
- records of any performance issues that you may be involved in or any complaints that you may raise;
- details of safety, health, environment, security, quality or issues raised by you or relating to you in one of our internal reporting systems – Unusual Occurrence Reports (UNORs) or Quality Observation Reports (QORs).

How long is the information retained for?

Legal retention periods and Nuvia UK's standards as stated in Section 3 above will apply.

5. Radiation workers for whom we provide an Approved Dosimetry Service

What information do we ask for, and why?

We will use your data in conjunction with your employer to keep track of your exposure to ionising radiation at work and keep you safe, as we are required to by law (Ionising Radiation Regulations 2017). Unless you opt-out, your data may also be used for scientific studies of the relationship between radiation and potentially radiation-linked diseases.

We will record your name, contact details at work, national insurance number, sex and date of birth, so we can contact you, if necessary, and inform your employer and the HSE about your dose record. We also record a history of your radiation doses including external doses measured by personal dosimeters and internal doses measured by air sampling, bioassay or in-vivo monitoring. We hold summary details of any occupational medicals you may have attended, but not including any clinical information, because we need to know that you are fit to work. And, if you tell us you are pregnant, we will record that information so your baby can be protected.

If your employer participates in the National Register of Radiation Workers or the UKAEA Mortality Study and you have not withdrawn from participation in those studies, we will send your data to the study organisers. If you die, or are diagnosed with a potentially radiation-linked disease, they will obtain that information from the NHS Central Registers and store it with your other data, so they can investigate any relationship between radiation and ill-health. This helps to improve the protection given to everyone working with radiation.

What is the legal basis for processing of personal data?

For the radiation dose data we hold, the legal basis for the processing is to comply with our legal obligations under the Ionising Radiation Regulations. In the case of participation in the scientific studies mentioned above, Public Health England is the data controller, and holds the data for reasons of public interest in the area of public health.

Who do we share the information with?

The data we hold, but not the data held by the NRRW or UKAEA Mortality Study, may be supplied to the following other organisations:

- Your employer, so they are aware of your radiation exposure and related information.
- The Health and Safety Executive, who have a legal right to the data for their Central Index of Dose Information.

- Other Approved Dosimetry Services who may provide support for your radiation protection, according to the legal requirements under the Ionising Radiation Regulations 2017.
- The Occupational Health service provider responsible for undertaking your IRR medical review.
- Public Health England, if your employer participates in the National Register of Radiation Workers and you have not opted out.
- Nuvia's SHIELD Database, if your employer participates in the UKAEA Mortality Study and you have not opted out.
- If you make a claim under the Compensation Scheme for Radiation Linked Diseases, your data will be shared with UKAEA and its agents.

The data about you held by the NRRW or UKAEA Mortality Study may be shared with the NHS Central Registers in a form in which you can be identified. Any other data sharing from those studies will be anonymised, so no individuals can be recognised. More information on the studies can be found here:

<https://www.gov.uk/government/publications/radiation-workers-and-their-health-national-study>.

Where there is a legitimate reason to send your data overseas, for example to your current or future employer, that transfer will be carried out following the guidance of the Information Commissioner.

How long is the information retained for?

The Ionising Radiation Regulations 2017 require us to keep your dose record for at least 30 years, but in practice we will keep it for much longer in order to deal with any Compensation Scheme claims you may make. The data about you held by the NRRW or UKAEA Mortality Study will be held for the duration of the studies.

It is a condition of employment as a radiation worker that we hold details of your radiation exposure. However, you can withdraw consent to participation in the NRRW or UKAEA Mortality Study at any time.

6. People who attend our radiation safety training courses

We provide radiation safety training courses for individuals from other organisations, and for reference purposes we retain details of the names of people who attended the courses, the organisation they were representing, and the results from the course.

7. Business contacts

We hold business contact details for clients and customers with whom we have a legitimate business relationship. We use these contact details to provide information to our clients and customers about our products and services, and any marketing events and activities. The contact list is periodically reviewed with the aim of ensuring that it is relevant and up to date, and you may let us know at any time if you no longer wish to receive these communications.

8. Visitors to our website

When someone visits www.nuvia.com we use a third party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website. If we do want to collect personally identifiable information through our website, we will be up front about this. We will make it clear when we collect personal information and will explain what we intend to do with it.

For information on how we use cookies on the Group website, see <https://www.nuvia.com/privacy-policy/>.

Security and performance

Nuvia uses a third-party service (Fasthost) to help maintain the security and performance of our website. To deliver this service it processes the IP addresses of visitors to the Nuvia website.

People who contact us via social media

In some circumstances, we use a third-party provider, Hootsuite, to manage our social media interactions. If you send us a private or direct message via social media the message will be stored by Hootsuite. It will not be shared with any other organisations.