

EMPLOYEE, WORKER AND CONTRACTOR PRIVACY NOTICE

Welcome to Newton's privacy notice which applies to all Newton employees, workers and contractors. We may update it at any time.

We need to collect and use certain information about you so that we can manage our relationship with you. Some information we collect and use will be personal data.

As you will know from Module 1 of our GDPR training course, personal data is any data which identifies you as an individual. It includes your name, address and phone number, but also appraisal information and your employment history.

Newton Europe Limited is the "data controller" and is responsible for your personal data (referred to as "Newton", "we", "us" or "our" in this privacy notice). This means that we decide how we hold and use personal information about you. Using your personal data allows us to schedule you to projects, provide you with IT equipment, and perhaps most importantly, to pay you!

Newton respects your privacy. We think that it is important to be transparent about how we collect and use your personal data and are committed to protecting the privacy and security of the information we hold about you. This privacy notice provides more information about how we do this and provides you with certain information that must be provided under the retained EU law version of the General Data Protection Regulation (**UK GDPR**).

This notice applies to all current and former employees, workers and contractors. It does not form part of any contract of employment or services contract, and we may update it at any time.

If the concepts introduced above about personal data aren't ringing a bell, please make sure that you have done the GDPR training course in N-Able. You can access the course [HERE](#).

If you have further questions about this notice, or about data protection or the security of your data, please contact David Audis (David.Audis@newtoneurope.com) or James Willison (James.Willison@newtoneurope.com).

1 DATA PROTECTION PRINCIPLES

We will comply with data protection law and principles, which means that your data will be:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes;
- accurate and kept up to date;
- kept only as long as necessary for the purposes we have told you about; and

- kept securely.

2 WHAT PERSONAL DATA DO WE COLLECT?

We collect, store and use a range of personal data about you. This includes the following:

- personal and work contact details, such as name, title, addresses, telephone numbers and email addresses;
- date of birth;
- gender;
- information about your marital status, next of kin, dependants and emergency contacts;
- recruitment information (including references, start and end dates with previous employers and other information included in a CV or cover letter or as part of the application process);
- information about your nationality and entitlement to work in the UK;
- if you require a visa to work for Newton, we or our appointed representatives may be legally required to obtain a great deal of information about you, about which you will be notified separately;
- copy of driving licence;
- copy of passport;
- photographs or videos;
- terms and conditions of your employment;
- current and previous employment records (including job titles, work history, compensation and compensation history, working hours, training records and professional memberships);
- details of your current and historical schedule (start date, project, days of work, working hours and work location) and attendance at work;
- reason for leaving and confidential references provided by us, alongside information required to provide reference information;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover and student loan information;
- results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied;
- bank account details, payroll records, tax status information and national insurance number;
- details of any payments made on termination;

- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, people scores, training you have participated in, performance improvement plans and related correspondence; and
- information about your use of our information and communications systems, including information obtained through electronic means such as key fob access.

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

- information about your race or ethnicity, religious beliefs, sexual orientation and political opinions/affiliation/political party membership;
- information about your health, including any medical condition, health and sickness records. Note that this expressly includes (but is not limited to) health data relating to Covid-19 testing;
- genetic information and biometric data; and
- information about criminal convictions and offences.

3 HOW IS YOUR PERSONAL DATA COLLECTED?

We collect personal information about you in a variety of ways. For example, from:

- you directly. For example, during interviews, meetings or assessments;
- forms or other correspondence provided by you. For example, application forms, your CV, or other forms completed at the start of or during employment;
- samples provided by you (in the context of Covid-19 testing); and
- your identity documents, such as your passport and/or driving licence.

We may also collect personal data about you from third parties, such as:

- your line manager or development manager;
- your named referees;
- employment agencies;
- the Disclosure and Barring Service in respect of criminal convictions;
- background check providers;

- credit reference agencies (as permitted by law); and
- publicly accessible data from third parties, including LinkedIn and Facebook.

We will also collect additional personal data in the course of job-related activities throughout the period of your working for us. For instance, if you complete an Equality and Diversity Monitoring form, this will reveal certain information about your race or ethnicity, whether you consider yourself to be disabled, your sexual orientation, religion and belief and gender monitoring.

Data is stored in a range of different places, including on your personnel file, in OneView, in our HR management systems and in other IT systems (including our email system).

4 WHY DO WE NEED TO PROCESS YOUR PERSONAL DATA?

We will need to collect, store and use personal data about you (and in some circumstances personal data about your family members or dependants) for a number of reasons:

- to **perform our obligations under your contract of employment**. For example, we need to process your personal data to pay you your salary and provide your benefits;
- to **ensure that we comply with our legal obligations**. For example, we are required to check your entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable you to take holiday;
- to **pursue legitimate interests of our own, or those of third parties**. When we do this, we always make sure that your fundamental interests and rights do not override those interests; and
- because **you have given your consent for us to do so**.

The examples given below do not form an exhaustive list of purposes for which your personal data will be processed, and we reserve the right to add to them at any time.

5 SITUATIONS IN WHICH WE USE YOUR PERSONAL DATA

The situations in which we will process your personal data are listed below:

To perform our contract of employment with you, including:

- deciding about your recruitment or appointment;
- determining the terms on which you work for us;
- paying you and, if you are an employee or deemed employee for tax purposes, deducting tax, National Insurance contributions and other relevant deductions (such as season ticket loans, student loans etc.);
- providing benefits to you, including: holiday, pension, private medical insurance (for yourself and/or family members, as applicable), life assurance, childcare vouchers, cycle to work etc. and inviting you to participate in and administering any share plans operated by us;

- liaising with our pension provider;
- administering the contract we have entered into with you;
- making decisions about salary reviews and compensation;
- assessing qualifications for a particular job, role or task, including decisions about promotions and other role changes;
- making decisions about your continued employment or engagement;
- making arrangements for the termination of our working relationship;
- management and planning, including accounting and auditing;
- ensuring that your wishes are met regarding death in service payments and that your next of kin are contacted in the event of an emergency; and
- enabling you to apply for flexible working or other family rights (for example, maternity, paternity, parental leave). This requires details of your partner/dependents.

To comply with our legal obligations, including:

- checking you are legally entitled to work in the UK;
- dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- ascertaining your fitness to work;
- managing sickness absence;
- complying with health and safety obligations;
- complying with our obligations to deduct taxes from contractors who fall within IR35 legislation;
- complying with our obligations to notify law enforcement about criminal activity or convictions;
- complying with our obligation to make reasonable adjustments for employees, workers and contractors who have a disability; and
- to prevent fraud.

To pursue legitimate interests of our own, or those of third parties, including:

- to provide and administer non-contractual employee benefits, such as N-Weekends. The legitimate interest is to ensure that you receive and we administer benefits which are not necessary for the performance of your contract; and

- personal data relating to education, training and development requirements, including personal data provided by you on training forms, booking request forms, conference application forms, various study and exam booking forms, supplier forms and training feedback forms (on paper or in N-Able). The legitimate interest is to ensure your continuing learning and development needs are addressed and documented;
- personal data obtained in relation to the performance and appraisal processes. The legitimate interest is to ensure your performance is assessed so that if there are improvements required they can be addressed and all levels of performance can be identified and, if appropriate, rewarded;
- to monitor your driving performance whilst using a company car. The legitimate interest is to protect the health and safety of our employees, contractors, candidates and clients;
- personal data obtained in relation to grievance and disciplinary issues. The legitimate interest is to address issues and concerns from either side in the employment relationship;
- to conduct data analytics studies to review and better understand employee retention and attrition rates. The legitimate interest is to better understand what we can do to improve retention and attrition rates;
- personal data obtained in relation to the monitoring of our IT systems. The legitimate interest is to ensure compliance with our IT policies and to ensure the integrity of our IT systems, to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- personal data obtained through access fobs. The legitimate interest is to ensure only authorised members of staff or authorised visitors enter our premises, thereby safeguarding systems and property from unauthorised access, destruction or theft; and
- Reference information. We generally provide only basic factual information about ex-employees (or departing employees) to prospective new employers. However, where we have legitimate concerns which, if not disclosed to a prospective new employer, could place Newton in breach of its duty of care to that prospective new employer, such information as Newton reasonably considers necessary will be disclosed in order to satisfy that duty.

Where you have given your consent. For example:

- Newton employees and contractors have the option of having their photographs and contact details uploaded to the Newton employee guide and “The Name Game” App so that people can put a name to a face and facilitate easier introductions. Use of your personal data on the employee guide and App is entirely voluntary and you can withdraw your consent at any time.

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

6 SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL CONVICTIONS

“Special categories” of personal data require higher levels of protection. Please refer back to Module 1 of the GDPR training course for more details.

We need to have further justification for collecting, storing and using this type of personal data. We may process special categories of personal data in the following circumstances:

- in limited circumstances, with your explicit written **consent**;
- where we need to carry out our **legal obligations**;
- where it is needed in the **public interest**, such as for Equality and Diversity monitoring (where such information is provided by you);
- where it is necessary to **protect you or another person from harm**;
- where it is needed to **assess your working capacity** on health grounds, subject to appropriate confidentiality safeguards; and
- less commonly, 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 will use your special categories of personal data in the following ways:

- 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 (including the results of Covid-19 testing), or disability status, to ensure your health and safety in the workplace and the health and safety of others and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits. We may obtain information relating to your physical and mental health from medical and occupational health professionals we engage and from our insurance benefit administrators; and
- we will use information about your race or national or ethnic origin, religious or other beliefs, or your sexual life or sexual orientation, to ensure meaningful Equality and Diversity monitoring and reporting.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about 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 may use information relating to criminal convictions where it is necessary as part of your role to undertake a DBS check prior to working in a particular area, 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.

7 IF YOU FAIL TO PROVIDE PERSONAL INFORMATION

You have some obligations under your employment contract to provide us with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide us with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable us to enter a contract of employment with you.

If you do not provide other information, this will hinder our ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

8 WHO HAS ACCESS TO YOUR PERSONAL DATA?

Your information will be shared internally, including with HR, recruitment, finance, talent, legal, scheduling, your line manager, your development manager, managers in your team and IT staff, in each case if and where access to the data is necessary for performance of their roles.

We may also share your personal data externally 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. For example, we may share your personal data with third parties in order to:

- obtain pre-employment references from other employers or referees;
- obtain employment background checks from third-party providers;
- obtain necessary criminal records checks from the Disclosure and Barring Service;
- obtain security clearance for you (if applicable);
- obtain training, coaching or other professional development services external providers;
- administer our payroll (including salary and expenses);
- provide benefits (contractual and non-contractual), including (but not limited to) running and administering internal and external events;
- report the outcome of Covid-19 testing to the Department of Health and Social Care as part of the NHS Test and Trace scheme, which is a condition of participation in their testing scheme;
- conduct analysis on our behalf. For example, analysis of our recruitment campaigns or Equality and Diversity monitoring; and

- provide occupational health services and our employee assistance and confidential helpline programmes.

Where we share your personal data with third parties, we require that they respect the security of your data and treat it in accordance with the law. 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.

9 INTERNATIONAL TRANSFERS

Many of our external third parties are based outside the United Kingdom (UK) so their processing of your personal data will involve a transfer of data to countries outside the UK.

Whenever we transfer your personal data out of the UK, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- we will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by virtue of an adequacy regulation under section 17A or adequacy decision under section 18(2) each of the DPA 2018; and
- where we use certain service providers, we may use standard clauses approved by the Secretary of State under section 119A of the DPA 2018 which give personal data the same protection it has in the UK; and
- where we use a service provider who is a member of a larger corporate group and this will involve the service provider transferring personal data outside the UK (but within their group of companies) the service provider may have binding corporate rules in place (checked and verified by us).

Please contact David Audis (David.Audis@newtoneurope.com) or James Willison (James.Willison@newtoneurope.com) if you want further information on the specific mechanism used by us when transferring your personal data out of the UK.

10 HOW DO WE PROTECT YOUR PERSONAL DATA?

We have put in place measures to protect the security of your information. Details of these measures are available upon request. For example, hard copy employee personal data is stored securely in locked cupboards by HR.

We have also put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

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.

Where we engage third parties to process personal data on our behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

11 FOR HOW LONG DO WE KEEP YOUR PERSONAL DATA?

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. After this period, we will securely destroy your personal information.

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

12 WHAT ARE YOUR RIGHTS?

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

- **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;
- **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;
- **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);
- **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;
- **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; and
- **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 HR in writing.

You will not have to pay a fee to access your personal information (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.

If you believe that we have not complied with your data protection rights, you can complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

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.

13 AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

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.

14 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 data.