DATA PROTECTION POLICY

What is personal information?

Personal information (sometimes called 'personal data') is any information that identifies and relates to a living person. This can include information that, when put together with other information, can then identify a person.

Because personal information allows people to know things about you, we need to protect this information and only use it for certain purposes.

Some information needs more protection. It might be information that you would not want widely known or that is very personal to you. This is sometimes also referred to as 'sensitive personal data' or 'special categories of data'. This would include anything that relates to your:

- Physical and sexual health
- Religious or philosophical beliefs
- Ethnicity
- Physical or mental health
- Trade union membership
- Political opinion
- Genetic/biometric data
- Criminal history

What personal information do we collect about you and what do we do with it?

Visitors to our websites

We collect standard internet log information and basic details of visitor behavior so that we can work out the cause of any problems with our websites. We collect this information in a way that does not personally identify you, so it is not personal information.

If we do want to collect personal information through our website, we will always tell you and will explain what we will do with the information you provide.

Use of cookies on our websites

Cookies are small text files that are placed on your computer by websites that you visit. They are used to make websites work (or work better) as well as to provide information to the owners of the site. We use cookies on our websites.

Read about the cookies we use on the link below;

https://www.sia.homeoffice.gov.uk/Pages/cookies.aspx

Registered Address: Unit J2, East Mill, Imperial Business Park, Gravesend, Kent DA11 0DP
0203 404 9744
info@nextrarecruitment.co.uk
Registration Number: 15666503

Market research

We conduct market research regarding the private security industry, and when we do, we may exchange your personal data with carefully selected third parties. This is permitted by Section 1 of the Private Security Industry Act 2001, which allows us to undertake, to arrange for or support the carrying out of research (which includes the exchange of personal data) relating to the provision of security industry services and of other services involving the activities of security operatives

Any personal data that is shared is securely destroyed immediately after any research has been completed

If you contact us via social media

If you send us a private or direct message via social media, it will not be shared with any other organisation.

Please note that all comments and messages, including direct messages, posted to our social media sites Facebook, Twitter or LinkedIn belong to the person posting.

We do not own or hold any of the data that individual's post. As a result, we are unable to delete this information. However, we do take steps to remove personal information so that it is not visible to the public

If you email us

We also monitor any emails sent to us, including file attachments, for viruses or malicious software. Please be aware that you have a responsibility to ensure that any email you send is within the bounds of the law.

When you phone us, you will be required to answer security questions so we can be sure you are who say you are.

If you make a complaint to us

When we receive a complaint about Nextra Recruitment, we make a file containing the details of the complaint. This normally contains the identity of the complainant and any other individuals involved in the complaint.

We will use the personal information we collect to process the complaint and to check on the level of service we provide. We do compile and publish statistics showing the number of complaints we receive, but not in a form which identifies anyone.

We usually must disclose the complainant's identity to whoever the complaint is about. This is inevitable where, for example, the accuracy of a person's record is in dispute. If a complainant does not want information identifying him or her to be disclosed, we will try to respect that. However, it may not be possible to handle a complaint on an anonymous basis

We will keep personal information contained in complaint files in line with our retention schedules. It will be retained in a secure environment and access to it will be restricted to those staff that require access for their role.

Right to work checks

We will check whether applicants have the right to work in the UK. To do this we will check the right to work of non-EU applicants with the Home Office. To do this we will send your name, date of birth, gender, and nationality details to the Home Office

Our staff

We collect a range of personal data about employee, agency, and contract staff to manage their employment relationship with us during the recruitment process, while they are working for us, at the time their employment ends and after they have left. Staff should see our Internal Data Protection Policy for more information regarding how we handle their data. Former staff should contact info@nextrarecruitment.co.uk to obtain a copy of our current Data Protection Policy.

Why we ask for your personal information

We will only ask you to provide personal information if we need it. Typically, when we collect the information, we will tell you why we need it, what we will do with it and whether we will share it with anyone else.

In general, we collect and use personal information where:

- It is necessary to perform our statutory functions under the Private Security Industry Act 2001 e.g., to operate our individual licensing or our approved contractor regimes, conduct market research regarding the private security industry or manage the business of our organisation.
- It is required by law e.g., to comply with employment law or health and safety legislation.
- We have a contract with you e.g., you work for us, you provide a service to us, or we have approved you to do something i.e., offer licence linked qualifications or conduct approved contractor assessments.
- You (or your legal representative) have given us your consent e.g., you signed up to receive marketing information from us, receive text messages from us or agreed to the use of cookies on our website.
- We will never sell your personal information to anyone else.

Who we share your personal information with?

We can only share information when the law tells us we can do so.

We share information with core service providers and third-party platforms as required for our business to function e.g., IT providers, payroll providers, pension scheme providers, auditors, legal advisors etc.

We also share and receive information we collect for our statutory purposes with other government agencies to:

- Conduct checks against our licensing or approved contractor criteria or conditions
- To check the accuracy of information we hold
- To prevent or detect crime.
- To protect public funds
- As otherwise permitted by law.

The agencies we typically share and receive personal information with relating to whether you are fit and proper to hold our SIA license are:

- The Home Office
- The Police
- The Department for Work and Pensions (DWP)
- Credit Safe
- Her Majesty's Revenue and Customs (HMRC)
- The National Crime Agency (NCA)
- Vetting agencies (the Disclosure and Barring Service (DBS), Access NI and Disclosure Scotland)

We will also share your personal information with any business you link your online account with.

The agencies we typically share and receive information within relation to whether you are fit and proper to join Nextra Recruitment:

- The Home Office
- The Police
- The Department for Work and Pensions (DWP)
- Her Majesty's Revenue and Customs (HMRC)
- Local authorities
- Payroll or finance companies associated with applicant businesses.
- Consultants acting on behalf of applicant businesses.

The agencies we typically share and receive information within order to manage our relationship with staff and prospective staff include:

- Home Office Departmental Security Unit
- Vetting agencies (the Disclosure and Barring Service (DBS), Access NI and Disclosure Scotland)
- UK Border Agency
- Occupational health providers
- Pay and Pension Providers

How we store your personal information

Most of the information we hold on you will be stored electronically. Even if you send us documents, we will usually scan these and then either return the originals to you or destroy them. Please see 'How do we protect your information?' for details of how we keep this safe.

How we protect your personal information

The security of your personal information is very important to us. There are several ways we make sure that the information we hold about you (on paper and electronically) is secure. We make sure that we only make this information available to those who have a legal right to see it.

Examples of our security include:

- Securely storing electronic information with appropriate encryption or security controls where required, both at rest and in transit in accordance with industry best practice and available technologies.
- Controlling access to systems and networks so that only those people who need to and can see your personal information and able to access it.
- Training for our staff to make sure that they know how to handle personal information and how and when to report when something goes wrong.
- Making sure we only discuss personal information with a data subject once we have confirmed their identity.

How long we store your personal information

How long we keep information you give to us depends on exactly what information it is, why we need it, and what we use it for. There will usually be a legal reason for keeping your personal information for a particular period. We try to include all of these in our retention schedule

For example, we will usually keep information you provide or that we collect in relation to applying for a job at Lexnis Group, we will application forms and personnel files you submitted to us for five years.

Transfers of your data outside the EU

We do not routinely transfer data outside of the EU. If we decide to store any other data outside of the EU, we will tell you before we do so.

Your rights

Data Protection law gives you rights about the personal information we hold and how we use it.

The right to ask for the information we hold on you

You have the right to ask for all the information we have about you. This is called a 'Subject Access Request'.

There is some information we may not be able to share with you. Some examples of this are:

- Information that is also about other identifiable people
- Information that might stop us preventing or detecting a crime if we were to share it

The right to ask us to change information you think is inaccurate.

You should let us know if you think information, we hold on you is out-of-date or inaccurate. We may not always be able to change or remove that information, but we will correct any factual inaccuracies and will include your comments in the record to show that you disagree with it.

There is some information you can update or correct without needing to contact us:

If you would like to ask us to change information, we hold on you that is not included above, use the 'Contact Us' form on our website.

The right to ask us to delete information (sometimes called 'the right to be forgotten')

In some circumstances you can ask for your personal information to be deleted, for example:

- Where your personal information is no longer needed for the reason why it was collected in the first place
- Where you have removed your consent for us to use your information and there is no other legal reason, we need to use it for
- Where deleting the information is a legal requirement

Where your personal information has been shared with others, we will do what we can to make sure those using your personal information comply with your request for erasure.

There are some circumstances in which we will not be able to delete information. For example:

- We are required to keep the information by law.
- Holding the information is required for us to carry out our statutory duties.
- Holding the information is required for the detection or prevention of crime.

If you would like to ask us to delete information, we hold on to you, please email info@lexnis.co.uk. Please reference the subject box 'The personal information we hold on you' and then the topic 'Ask us to delete information'.

The right to ask us to limit what we use your personal data for

You have the right to ask us to restrict what we use your personal information for if:

- You have identified inaccurate information and have told us about it.
- We have no legal reason to use that information, but you want us to restrict what we use it for rather than erase the information altogether.

When information is restricted, it can be stored but it cannot be used without your consent, other than to handle legal claims and protect others, or where it is in the public interest.

There are some circumstances in which we will not be able to limit how we use your information. For example:

- We are required to use the information by law.
- Using the information is required for us to carry out our statutory duties.

- Using the information is required for the detection or prevention of crime.

If you would like to ask us to limit how we use information we hold on you, use the 'Contact Us' form on our website.

The right to ask for your personal information to be moved to another agency (knows as 'Data Portability').

You can ask for your personal information to be given back to you or another service provider of your choice in a commonly used format.

This only applies if we are using your personal information with consent (not if we are required to by law) and if decisions were made by a computer and not a human being.

It's likely that data portability won't apply to information we hold on you, but If you would like to ask us to move your information to another agency, use the 'Contact Us' form on our website.

What to do if you have questions or concerns

If you have questions about how we collect, use, or store your personal information, or your rights, please contact our Data Protection Officer, info@nextrarecruitment.co.uk

For independent advice about data protection, privacy, and data sharing issues, you can contact the Information Commissioner's Office (ICO).

You can visit the ICO website at www.ico.org.uk or email them at casework@ico.org.uk

Changes to this Privacy Policy

We keep our Privacy Policy under regular review. This privacy notice was last updated on 25 May 2020.

Who is the data controller?

Nextra Recruitment Limited is the data controller.

You can contact us by writing to:

Head Office, Unit J2, East Mill, Gravesend, DA11 0DP

0203 355 5392

info@nextrarecruitment.co.uk

Director: 

Registered Address: Unit J2, East Mill, Imperial Business Park, Gravesend, Kent DA11 0DP
0203 404 9744
info@nextrarecruitment.co.uk
Registration Number: 15666503