Candidate Privacy Notice

Classification: General

Candidate Privacy Notice Version 1.5

We're committed to protecting your rights and freedoms with regards to your personal data. This notice describes how we collect, store, use, and share personal information. It also explains the rights you have in relation to the personal information that we hold about you.

This notice is applicable to all candidates globally, both those applying for permanent and fixed term roles. It applies to agents and contractors, as well as other roles such as interns, trainees and graduates who work on an NCC Group project.

Where you submit information about others such as people who may provide personal references, we'll explain how their information will be used. Please make sure that they're aware of this.

Please note that we have layered this Notice in order to simplify the content, which is in accordance with good practice guidance issues by the EU Data Protection Regulators. This mean we have embedded links to further information at the appropriate point, to ensure this is easily accessible. We have checked these links are authentic prior to publication.

As of the 31st January 2020, the UK is no longer part of the EU. Hence the EU's GDPR no longer applies. However, the UK government has directly translated the EU GDPR into UK law. Therefore, all requirements remain the same, and all references to the GDPR relate to both the UK and EU regimes.

Who we are

When we say 'we' or 'us' in this notice, we're referring to NCC Group plc, a company registered in England and Wales (registered number 04627044) whose registered office is at XYZ Building, 2 Hardman Boulevard, Spinningfields, Manchester, M3 3AQ.

Within NCC Group additional entities are employers, so will also process your personal data as 'Data Controllers'. Please see your contract for the applicable entity, which includes;

- Australia – NCC Group PTY Limited
- Canada – NCC Group Security Services Corporation
- Denmark – NCC Group A/S
- Germany – NCC Group GMBH
- Japan – NCC Group Japan K.K
- Netherlands – Fox-IT B.V, Fox – IT Crypto B.V. NCC Group Escrow Europe BV
- Singapore - NCC Group Private Limited
- Spain – NCC Group Security Services España S.L.
- Sweden – Cyber Assurance Sweden AB
- Switzerland – NCC Group Escrow Europe (Switzerland) AG
- Portugal – NCC Group Cyber Security Portuguesa Unipessoal LDA
- United Arab Emirates – NCC Group FZ-LLC
- UK - NCC Group Security Services Limited, NCC Services Limited, NCC Group Corporate Limited
- US – NCC Group Security Services Inc, NCC Group LLC, NCC Group Escrow Associates LLC, Payment Software Company Inc, Virtual Security Research LLC, NCC Group Software Resilience (NA) LLC

What kinds of information do we collect about you?

We're subject to a variety of legal regimes, so the personal data we collect will vary from country to country. To make sure this privacy notice is clear for everyone, we've summarised the types of personal data below, and called out the main differences;

- Personal - such as name, date, and place of birth, contact numbers, email, address, picture. We collect marital status in some countries upon appointment, and in the US we will note if

you're from a latino background or if you're a veteran.
- Education and training - qualifications, training records and any professional certifications relevant to your role.
- Job-related - such as references, CVs, screening outcome, start date, department, line manager, salary, benefits.
- Conflict of interest information – such as details of investment portfolios and / or other positions. This will only be for specific high risk roles.
- Government identification – such as passports, national ID cards, driving licences or other permits.
  Citizenship and diversity – such as race & ethnicity, sex assigned at birth, gender identity, sexual orientation, disability, neurodiversity and pro-noun. We will only ask for this information in countries where we have a legal basis to do so.
- Referees (people who provide references for you) – we'll only use their information to obtain the references, and will retain copies on your file.
- Call recordings, CCTV footage and Building Access logs – such as if you have an assessment with our Sales Team (where calls are recorded), or when you attend any of our premises.
- Candidate feedback forms about our recruitment process and work experience forms if you wish to be contacted about future opportunities at NCC.

Why do we use your personal information?

We keep personal information about you in order to administer our recruitment processes and to allow us to improve our processes. This includes for:

- Recruitment
- Screening
- HR administration / payroll
- Identity checks
- Ad hoc / by exception for legal defence, or in an emergency situation
- Equalities monitoring
- Analysis and management reporting
- Call recordings
- CCTV
- Website monitoring

Where do we get your information from?

As well as receiving information directly from you, your references, and your hiring manager, we also obtain information from;

- LinkedIn, when you apply for a role via LinkedIn or other means, or where we are proactively searching for candidates. We can see full profiles and contact details unless you have changed your LinkedIn settings. Please see the LinkedIn Privacy Policy for more.
- Recruitment agencies.
- Internet searches / job boards.
- Social Media channels such as Twitter and GitHub, where we will make or keep in contact with potential candidates.
- Events / networks / lectures.
- Technical competitions and challenges.
- Referrers, i.e. employees who refer a candidates for a role.

Depending on the applicable screening practices in your country, we may collect information from other sources;

- Screening provider – the service may involve the provider requesting data from the Police, past employers and other relevant third parties.
- Government departments – for example driving licence authorities to check you are safe to drive on business. Fox IT's screening process may involve government or military departments – with the level of screening depending on the position / department / responsibilities.

Where we obtain such information, we'll look to make sure you're informed in advance – for example as part of your contract and privacy notices within screening forms, and we also publish this privacy notice on our website.

How do we use your personal information, and what are our legal grounds?

Worldwide, a number of Data Protection laws require organisations to process personal information only where we have a 'lawful basis.' This section will explain the legal basis/es applicable in your country.

Please make sure you read the 'Use of your Information' column below regardless of your location.

Australia

- Consent is required for diversity information.
- (A legal basis is not required for non-sensitive information.)

Canada

- Consent is required for diversity information.
- A legal basis is not required for non-sensitive information

Japan

- Consent is **not** required for transfers to the UK / EU (where a lot of employee data is stored), or for transfers to providers of outsourced services (such as Workday).
- Consent is required for diversity information.
- A legal basis is not required for non-sensitive information)

Singapore

- We use the employment conditions for collection and use of your data.
- Consent is required for diversity information.

US

- Consent is required for diversity information.
- For non-sensitive information for our business purposes

Netherlands

- Consent is required for diversity information.
- For non-sensitive information we will rely on performance of a contract, or necessary steps in order to enter into a contract with you.

Denmark

- For non-sensitive information we will rely on performance of a contract, or necessary steps in order to enter into a contract with you.

Belgium

- For non-sensitive information we will rely on performance of a contract, or necessary steps in order to enter into a contract with you.

United Kingdom

- Consent is required for diversity information.
- For non-sensitive information we will rely on performance of a contract, or necessary steps in order to enter into a contract with you.

Germany

- For non-sensitive information we will rely on performance of a contract, or necessary steps in order to enter into a contract with you.

Spain

- Consent is required for diversity information.
- For non-sensitive information we will rely on performance of a contract, or necessary steps in order to enter into a contract with you.

Portugal

- Consent is required for diversity information.
- For non-sensitive information we will rely on

performance of a contract, or necessary steps in order to enter into a contract with you.

Where we process your personal data based on consent as within your local data protection law, it is worth noting that this is **not the same** as consent under the GDPR. The requirements for GDPR-standard consent means this can only be used in very specific circumstances, and it is unlikely to be applicable to employees.

Where we are using non-GDPR standard consent, we will imply your consent by way of you entering into a contract with us, and will make sure the consent is informed by way of providing you with this notice. However please note that if you withdraw your consent, then we may not delete your data if we have a good reason for keeping it.

Below you can see more detail on legal bases under the General Data Protection Regulation;

Use of your information	Legal ground
Website monitoring We use consent to set and access cookies, when you visit our websites. See our Cookie Policy for more information.	Consent Your personal information may be processed when we receive your consent. The consent you provide must be freely given, informed, specific, unambiguous and be given with a positive affirmative action. Your consent can be withdrawn at any time.
Recruitment Our Talent and Recruitment teams post adverts and search for candidates. They collect applicants' names, contact details and CVs / details of relevant work experience, education and skills / LinkedIn profiles (as appropriate for the application method), and review these for suitability to create a short-list. This initial screening may involve a phone call to aid this initial screening, and / or to answer any questions you may have. In order to reduce unconscious bias, the Team may de-identify applications before sharing the short-listed candidates with the hiring manager. The manager then selects those they'd like to interview, at which point the Talent Team will always share identifiable CVs and LinkedIn profiles. The interview process may involve more than 1 step. Screening For some roles, NCC Group may need to carry out screening / vetting. This may include requesting references from previous employers and individuals who can verify your identity and / or skills and experience (we will explain the relevant process before proceeding). In the UK,	Necessary for the performance of a contract Your personal data may be processed when it's necessary in order to enter into or perform a contract.

we engage the services of a security screening company to carry out vetting, or in other countries we often do this ourselves. Where your role requires security screening, you will be required to undergo this process as a requirement of your employment contract. This screening is proportionate to make sure we comply with legal requirements and to make sure you're not susceptible to outside pressures which could compromise us. We will only obtain and further process criminal conviction information where this is authorised by national law; for example, through an established national criminal record vetting process. In Canada, screening providers aren't used so the process involves you obtaining a criminal record check yourself from the RCMP / Policy. Note only the screening date and date of next screening is stored in Workday. In the UK, as we use a screening company we don't get the specific details of screening, only the outcome. In countries where we do our own screening (which may just be employment references or may include credit reference / police record checks depending on the role), we store the personal data processed in order to conduct the screening within your local HR Team.	
Identity checks We request copies of official identity / registration documents (passport, ID card, driving licence etc. as acceptable in your country) – in the UK this is when we want to make an offer of employment (we need to see these before we issue the offer), or in the US this would be on your first day of work. We may take copies of these documents to verify an individual's identity, and their right to work in the location where you would be working, or we may just need to document we've seen these (in the US we attest to this using an I-9 form). Please only send us such details via a secure method – normal email is not secure for transferring sensitive information such as ID documents, but we can provide a secure portal where needed. Ad hoc We may disclose or share your personal data in order to comply with any legal obligation such as a court order.	Necessary for compliance with a legal obligation Your personal information may be processed in order to meet any legal obligations NCC Group is subject to.
By exception We may disclose your information to the police or other authorities if we have serious concerns about you or another's wellbeing.	Necessary to protect vital interests This will usually only apply in 'life-or-death' scenarios.
Equalities monitoring We collect and process diversity data to monitor equality of opportunity	Consent Your personal information may be

within NCC Group businesses. We will use this information to produce aggregated statistics about staff members in order to promote equality. These statistics will not allow individuals to be identified, and only your local HR team are able to see this information – the central (UK) team can report on this in aggregated form only. In countries where we collect this data we are able to do so with your consent. However **regardless of your location, the provision of equality data is not a statutory or contractual requirement, and is entirely voluntary. There are no consequences if you decide not to provide this information.**	processed when we receive your consent. The consent you provide must be freely given, informed, specific, unambiguous and be given with a positive affirmative action. Your consent can be withdrawn at any time.

Necessary for legitimate interests

We also use your information when we have a 'legitimate interest' and that interest isn't outweighed by your privacy rights. Each activity is assessed and your rights and freedoms are taken into account to make sure that we're not being intrusive or doing anything beyond your reasonable expectation.

We'll assess the information we need, so we only use the minimum. If you want further information about processing under legitimate interests you can contact us using the details below.

You also have the right to object to any processing done under legitimate interests. We'll re-assess the balance between our interests and yours, considering your particular circumstances. If we have a compelling reason we may still continue to use your information. We use legitimate interests for the following:

Use of your information	Legitimate interest(s)
Recruitment Our Talent Teams participate in a variety of events / networks / lectures including hacking challenges, job fairs at universities Candidate feedback forms, work experience forms etc. When we do so, we may collect your CV or contact details if you're interested in working for us now or in the future – in the UK we just collect details to allow us to connect on Social Media, whereas in Fox IT we keep more information. For candidates in other Countries, please reach out to your local Talent and HR contacts for more information.	We need to attract candidates who have the talents which will enable us to meet our commitments to our clients and develop our business.
Assessment We may use a range of psychometric assessments in our selection process, including personality and cognitive ability tests. These assessments have been designed and validated by experts in the field and have been shown to be reliable and effective in predicting job performance. We may also use other types of assessments,	We need to use assessments for candidates in our recruitment process to support the quality and fairness of our decision making and to reduce unconscious bias and improve consistency.

depending on the requirements of the role and the nature of the organization.	
Analysis and management reporting We analyse and report on our recruitment activities. Where we do so, we do this to produce aggregated reports – i.e. facts and figures, which no longer contain personal data. Any monitoring of individuals would only take place as part of a compliance monitoring assessment or an investigation. Key KPIs which are analysed relate to the time to hire, agency fees / savings, stakeholder satisfaction and hiring against business objectives.	We need to analyse and assess our recruitment performance in order to optimise our resources and ensure we're recruiting the right people promptly. We need to make sure we're appropriately allocating our resources and that our travel (e.g. to industry events and recruitment fairs) is cost-effective.
CCTV NCC Group buildings are monitored by CCTV cameras. Note that in some countries, we do have legal obligations to process CCTV such as the ABDO law in the Netherlands.	We need to ensure the safety and security of NCC Group staff, customers, and other visitors.

Who do we share your personal information with?

We share your personal data with other organisations. Who we share your personal data will depend on the job you have applied for and which location you are in. The organisations we share personal data with are as follows;

- Screening providers (which will include the Police and government departments / agencies for some Fox IT staff).
- Systems providers such as Workday, our financial management and human capital software provider.
- Government bodies and Regulators such as UWV, HMRC, the Health & Safety Executive (HSE), Federal Trade Commission, data protection regulators worldwide.
- Professional services providers and consultants where warranted, such as contractors, external search and assessment partners, external auditors and lawyers.

Providers as relevant to your role, such as health providers. For example our third party occupational health provider Bupa in the UK may be consulted on making adjustments.

We will always ensure that personal data will only be shared where there is a requirement to do so, and where appropriate technical, organisational, and where necessary, contractual measures are in place in order to ensure its protection.

Overseas transfers

The data that we process about you may be transferred to, or stored at, a destination outside the UK and / or European Economic Area ("EEA"). It may also be processed by staff operating outside the UK / EEA who work for us or for one of our suppliers.

We need to have legal grounds to transfer your data outside of the UK / EEA. Some countries have been assessed by the EU as being 'adequate', which means their legal system offers a level of protection for personal information which is equal to the EU's

protection. The EU Commissioner (and the Information Commissioner's Office for the UK) has also approved Binding Corporate Rules (BCRs) as an adequacy mechanism. This requires the company to commit to European data protection standards and provide oversight mechanisms, but BCRs are approved for a group of companies, in conjunction with all EU supervisory authorities, and require extensive monitoring and oversight before the BCRs are authorised.

Where the country or mechanism hasn't been assessed as adequate, the method we use most frequently is Standard Contractual Clauses (SCCs). The European Commission has recognised SCCs as offering adequate safeguards to protect your rights and we'll use these where required ensuring adequate protection for your information. The European Commission approved standard contractual clauses are available here.

We have SCCs in place to allow sharing between NCC Group entities globally. For our service providers, we make sure we have contract terms and make checks of their control environments to ensure that your data is treated compliantly, securely and in accordance with this privacy policy.

The main transfer of your personal data will be to Workday. The data is stored within the EEA – in Ireland and the Netherlands - however if we need specialist support on a change or initiative, there may be some remote access by Workday or other application management specialists in the US. We have SCCs in place in our contract with Workday, but they are also signatories to the EU-US Privacy Shield and have BCRs. We have also conducted extensive due diligence on Workday's controls.

If you're based in a country outside of the EEA, there may be local obligations with regards to the transfer. See below for details of the controls which we will apply to satisfy these;

- Australia – contractual commitments to comply with the Privacy Principles.
- Canada – clear privacy notices explaining the transfer. We also need to tell you who to contact for more information. Please contact the Data Protection and Governance Team as per the Contact section below.
- Japan – the UK and the EU are classed as adequate, so there are no obligations in relation to such transfers. For any other transfers, we ensure the recipient has established similarly adequate standards for privacy protection as specified in the Act on the Protection of Personal Information.
- Singapore – standard contractual clauses & BCRs are approved mechanisms.
- US – n/a - no restrictions around overseas transfers in the US.

How long do we keep personal information for?

Unless otherwise set out in this Privacy Notice, any information we process about you will be retained by us until we no longer need it for the purposes for which it was collected, as set out in this Privacy Notice. We will base that decision on criteria, including;

- Any legal or regulatory requirements to delete or retain the data for a specific timeframe,
- Our legitimate business reasons for keeping the data, such as to analyse and assess our activities. This includes assessing the fairness of our recruitment practices,
- The likelihood of a claim arising where we'd need to defend our conduct, and;
- Whether the data is likely to remain up to date.

We will review and delete or destroy personal data on a regular basis. If we are unable, using reasonable endeavours, to delete or destroy personal data we will ensure that the personal data is encrypted or protected by security measures so that it is not readily available or accessible by us.

Automated decisions / profiling

We may use psychometric testing in our recruitment process to make an automated decision about whether to progress individuals to the next stage of our recruitment process in the event that there are a large number of candidates for a role. An automated decision will be made based on the results of tests which measure relevant skills such as analysis aptitude, comprehension aptitude, technical aptitude, and workplace English. We will inform you before you complete a psychometric test if automated decision making will be used in the application process and explain how to request that the automated decision is reviewed by a human.

Your rights under the General Data Protection Regulation

There are a number of rights available under the General Data Protection Regulation (GDPR). These don't usually require any fee, and require us to respond within 1 calendar month in most circumstances. Not all rights apply in all situations, but for clarity we have not included full details here.

The easiest way to exercise any of your rights,or enquire if a right is applicable in a specific circumstance, would be to contact our Data Protection and Governance Team using the contact details below. If we need further information to comply with your request we'll let you know.

If you are not based within the EEA, the Data Protection and Governance Team will assess your request based on our ability to provide for your rights rather than your location.

Access to your data

You have the right to ask for access to and receive copies of your personal data. You can also ask us to provide a range of information relating to our processing of your data.

Rectification of your data

If you believe personal data we hold about you is inaccurate or incomplete, you can ask us to correct that information.

Right to be forgotten

In some circumstances, you have the right to ask us to delete personal data we hold about you.

Right to restrict processing

In some circumstances you are entitled to ask us to restrict processing of your personal data. This means we will stop using your personal data but we don't have to delete it.

Data portability

You have the right to ask us to provide your personal data in a structured, commonly used and machine-readable format so that you are able to transmit the personal data to another data controller.

Right to object

You are entitled to object to us processing your personal data if the processing is based on legitimate interests and/or is for the purposes of scientific or historical research / statistics.

If you would like to exercise any of your rights in respect of your personal data, please contact dataprotection@nccgroup.com or write to us at XYZ Building, 2 Hardman Boulevard, Spinningfields, Manchester, M3 3AQ.

Changes to this Privacy Notice

Any changes we may make to the Candidate Data

Privacy Notice in the future will be posted on this page and, where appropriate, notified to you by email. Please check back frequently to see any updates or changes.

Contact

Our Chief Data Protection & Governance Officer can be contacted using the following email address: dataprotection@nccgroup.com, or alternatively by writing to XYZ Building, 2 Hardman Boulevard, Spinningfields, Manchester, M3 3AQ.

Questions, comments and requests regarding the Colleague Privacy Notice are welcomed and should be addressed to dataprotection@nccgroup.com.

If you have any concerns about the ways in which we process your personal data, you have a right to complain to the relevant supervisory authority in your jurisdiction. We'd encourage you to contact us first, so we can address your concerns.

Please see below for details of the relevant regulators;

- Denmark
  - Datatilsynet
  - T: 33 19 32 00
- Germany
  - Bayerisches Landesamt für Datenschutzaufsicht
  - 0981 1800930
- Netherlands
  - Autoriteit Persoonsgegevens
  - T:070 888 8501
- Portugal
  - CNPD
  - T (+351) 213 928 400
- Spain
  - Agencia Española Protección de Datos
  - T: 901 100 099 / 91 266 35 17
- Sweden
  - Swedish Authority for Privacy Protection (IMY)
  - T: 08-657 61 00
- Switzerland
  - Schweizerische Eidgenossenschaft
  - T: 058 462 43 95
- UK
  - Information Commissioner's Office (ICO)
  - T: 0303 123 1113