GOVERNANCE

nccgroup

CANDIDATE PRIVACY NOTICE

NCC Group Candidate Privacy Notice

Introduction

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 data during your application procedure and after it ends. It also explains the rights you have in relation to the personal data that we hold about you. Please ensure that you read this notice (sometimes referred to as a 'privacy notice') and any other similar notice we may provide to you from time to time when we collect or process personal data 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 in this notice how their information will be used. Please make sure that they're aware of this.

All references to the General Data Protection Regulation (GDPR) relate to both the European Union (EU) and United Kingdom (UK) regimes.

If you are offered and you accept a role at NCC Group, the Candidate personal data collected during the recruiting process will become part of your employee file and will be governed by our Colleague Privacy Notice, a copy of which will be provided when you are onboarded as an employee or can be requested from your Talent Acquisition Partner.

Back to top

Who we are

When we say 'NCC Group,' 'we' or 'us' in this notice, we're referring to the group of companies collectively known as NCC Group, which are part of a structure managed by 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, United Kingdom.

NCC Group is a global business and even though you may be based in a country that is outside of the scope of the GDPR our approach globally is to align to this regulation as good practice. We believe this sets a high standard across the whole of NCC Group, aligns to the legislation within the jurisdictions that we operate in, and enables us to implement processes to protect personal data whilst still taking into account local variance.

NCC Group gathers and uses certain information about you. The NCC Group entity with whom you are interacting with will be the controller within the meaning of the GDPR. In most cases this will be NCC Group Corporate Limited, based in the United Kingdom, or aligned to where you are applying for a role:

- Australia – NCC Group PTY Ltd
- Netherlands – Fox-IT BV, NCC Group Escrow Europe BV
- Philippines – NCC Group Asia, Inc
- Singapore - NCCGroup Private Limited
- Spain – NCC Group Security Services España SL
- United Kingdom - NCC Group Security Services Ltd, NCC Services Limited
- United States - NCC Group Security Services Inc, NCC Group LLC, NCC Group Escrow Associates LLC, Payment Software Company Inc, NCC Group Software Resilience (NA) LLC

Some of our support functions, may be in a different country to you, for example, Human Resources or Information Technology. To facilitate this, we have a group wide Intra Group Agreement that protects transfers of personal data internally to the group.

Back to top

What kinds of information do we collect about you?

Under the GDPR, **personal data** refers to any information that relates to an identified or identifiable individual, such as names, contact details, and other information that directly or indirectly could lead to identification. **Special category data** is a subset of personal data that requires extra protection due to its sensitive nature. This includes data on racial or ethnic origin, political opinions, religious beliefs, health, sexual orientation, or biometric data. Processing special category data is subject to stricter conditions under the GDPR, such as specific consent or a legal (employment) obligation. Other jurisdictions may prescribe other types of sensitive data and conditions.

NCC Group is a global business and as a result the personal data we collect about you will vary depending on a number of factors:

- Your location of residence
- Your specific role
- The legal regime your specific NCC Group employing entity is subject to

The categories of personal data we process include, but are not limited to, those listed table below, with illustrative examples of the type of data that falls under each category. Local variations to this list, including local interpretations of the required level of protection with regard to sensitive data, are detailed at the end of this document.

If you would like to check specific collection for your individual circumstances, please speak to your Talent Acquisition Partner or contact dataprotection@nccgroup.com.

Category	Examples
Personal	Name, date of birth, contact numbers, email, address, gender, image. Marital status on appointment where it is required for your benefits.
Education and training	Qualifications, training records and any professional certifications or memberships, psychometric testing results, as relevant to your role.
Job related	References, CVs or job applications, screening outcome, start date, department, line manager, salary and benefits.
Conflict of interest information	Details of investment portfolios and / or other positions where this is required for specific roles.
Official government documentation	Passports, national ID cards, driving licences, visas or other required permits.
Diversity information	Pronoun(s), sex assigned at birth, race and ethnicity, sexual orientation, gender identity, disability status. This category describes the type of information we may collect; however, this varies according to local legislation.
Referees	Contact name, relationship to you, contact numbers, email, address.
CCTV & building access information	CCTV footage, building access logs if you attend any of our premises as part of the recruitment process.
Audio and visual recordings	Some calls may be recorded, such as interviews under specific circumstances where it is useful or appropriate to do so with your consent.
Candidate feedback	Feedback forms and other notes about our recruitment processes and work experience forms, a record of your preferences for contact regarding future opportunities at NCC Group.

Category	Examples
Screening data	The results of background checks as required for your role, potentially including personal, professional, and/or financial checks. The specific checks carried out will vary by country and legislation.
Nationality and immigration status	Details of your nationality and immigration status to establish your right to work and pay tax correctly.

Back to top

Where do we get your information from?

Most of the information we receive we obtain directly from you, through your references, and your hiring manager.

We may also receive data from additional third parties as and when this is required based on individual circumstances and where this is permitted by applicable laws.
Examples of these are:

- Recruitment agencies
- Job boards
- LinkedIn when you apply for a role through this method
- LinkedIn 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 information.
- Social Media channels, to make or keep in contact with potential candidates.
- Events / networks / lectures.
- Technical competitions and challenges.
- Referrers, such as those who refer a candidate for a role.
- Previous employers or personal references

Back to top

Why do we collect and how do we use your personal data?

Worldwide, there are many pieces of data protection legislation and regulation prescribing the processing of personal data. As NCC Group, we globally join the legal framework of the GDPR, as the personal data of candidates may be processed within the jurisdiction of the GDPR, but also as a commitment to good practice.

We use the personal data we collect from and about you only for the purposes described in this Privacy Notice or for purposes we explain to you at the time we collect your data. Depending on our purpose for collecting your personal data, we rely on one of the following legal bases:

- **Consent** - in certain circumstances, we may seek your consent (separate from any agreement between us) before collecting, using or disclosing your personal information. Where consent is used: It is voluntary and withdrawable at any time and there will be no negative consequences for not consenting or withdrawing consent.
- **Legal obligation** - we may need to process and retain your personal data to comply with the law or to fulfil certain legal obligations such as regarding occupational health and safety, or taxes.
- **Legitimate interest** - we will use or disclose your personal data for the legitimate interests of either NCC Group or the (compatible) derivative legitimate interests of a third party, such as our suppliers, but only when we are satisfied that your rights will be adequately protected.

If the processing of data is based on a legitimate interest, this requires a balancing test: identifying the legitimate interest, checking necessity of the processing activity, and balancing it against the individual's interests, rights and freedoms. For more information on the reasoning behind relying on the legal basis of legitimate interest per data processing activity, please see the table. If you require more information on how we assess our legitimate interest by use of the balancing test on a case-by-case basis, please reach out to the Data Protection & Governance team via dataprotection@nccgroup.com.

The following table provides more information on our purposes for processing your personal data and the corresponding legal bases. The legal basis on which your personal data are processed depends on the personal data in question and the specific context in which we use them.

Country specific variances are listed at the end of this document.

Back to top

How we use your personal data	Applicable categories	Performance of a contract	Legitimate interest	Legal obligation	Consent
Recruitment: orientation phase Our Talent and Recruitment teams post adverts and search for candidates. Personal data is collected during this process through CVs, applications and through LinkedIn profiles. The initial screening phase may also involve a phone call, emails or messages to aid this initial screening, and/or to answer any questions you may have. From this a shortlist is created and shared with the hiring manager and/or interview panel. To reduce unconscious bias, the Team may de-identify applications before sharing short-listed candidates with the hiring manager. The manager then selects those they'd like to interview, at which point the Talent Team share identifiable CVs and LinkedIn profiles with the hiring panel.	Personal Education and training Job related Conflict of interest information Referees Nationality and immigration status		✓		✓ (Philippines only)
		Philippines - Consent will be gained for educational background and criminal conviction information.			
Diversity monitoring If directly and voluntarily provided by you, we will collect Diversity Data to monitor the effectiveness of diversity and inclusion initiatives across the organisation. We will use this information to produce aggregated statistics about candidates to promote equality and for benchmarking.	Personal Diversity information				✓

How we use your personal data	Applicable categories	Performance of a contract	Legitimate interest	Legal obligation	Consent
These statistics will not allow individuals to be identified. **The provision of equality data is entirely voluntary. There are no consequences if you decide not to provide this information.**					
Recruitment events 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 information to contact you if you are interested in working for us now or in the future. This can be through different methods, such as collecting your contact details, CV, or by interacting with a link/QR code to sign up to be contacted by us.	Personal Job related		✓		
		We need to attract candidates who have the talents which will enable us to meet our commitments to our clients and develop our business.			
Website monitoring We use consent to set and access cookies when you visit our websites. See our Cookie Policy for more information.	Personal				✓
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	Personal Education and training		✓		

How we use your personal data	Applicable categories	Performance of a contract	Legitimate interest	Legal obligation	Consent
effective in predicting job performance. We may also use other types of assessments, depending on the requirements of the role and the nature of the organisation.					
		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.			
Screening For some roles, NCC Group may need to carry out screening or vetting. This may include requesting references from previous employers and individuals who can verify your identity and/or skills and experience. The relevant process for the country will be explained with you before proceeding. 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. Additionally, NCC Group may also engage a third party to perform a screening on the candidate. Please note that NCC	Personal Education and training Nationality and immigration status Government issued identification Referees Screening data		✓		✓ (Philippines only)

How we use your personal data	Applicable categories	Performance of a contract	Legitimate interest	Legal obligation	Consent
Group will not process any personal data in that regard, except for any general "points of concern" as fed back by that third party. That means that only the screening date, status and date of the next screening is stored in our HR system.					
Identity checks We request copies of official identity / registration documents as acceptable in your country. 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. These are sent via a secure method - we can provide a secure portal where needed for candidates.	Personal Official government documentation Nationality and immigration status			✓	✓ (Philippines only)
		Philippines - Consent will be gained for government issued identifiers.			
Analysis and management reporting We analyse and report on our recruitment activities. Where we do so, we do this to produce aggregated reports (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.	Personal Candidate feedback		✓		
		We need to analyse and assess our recruitment performance in order to optimise our resources and ensure we recruit the right people promptly. We need to make sure we're appropriately allocating our resources			

How we use your personal data	Applicable categories	Performance of a contract	Legitimate interest	Legal obligation	Consent
		and that our travel (e.g. to industry events and recruitment fairs) is cost- effective.			
Safety, Physical Security and Maintenance NCC Group buildings are monitored by CCTV cameras and access logs may be processed. We will collect footage from CCTV cameras and details of access from building access logs to ensure that only authorised persons are entering our premises, and in some cases to provide evidence during a disciplinary process.	Personal CCTV & building access information		✓		
		We need to ensure the safety and security of NCC Group staff, clients, and other visitors. CCTV and security monitoring must always adhere to the principles of proportionality and transparency. This means that data collected must be limited to what is strictly necessary for the intended purpose, avoiding excessive or irrelevant processing and data subjects should be clearly informed, ensuring openness and accountability in all data handling practices. If you require more information on the balancing test on a case-by-case basis, please reach out to the Data Protection and Governance team via *dataprotection@nccgroup.com*.			
Complying with court orders and other legal obligations We may disclose or share your personal data to comply with any legal obligation such as a court order.	Personal			✓	

How we use your personal data	Applicable categories	Performance of a contract	Legitimate interest	Legal obligation	Consent
Medical Emergencies We may disclose your information if we have serious concerns about you or another's wellbeing.	Personal				✓
		Or vital interests: Where there is a 'life-or-death' scenario.			

Who do we share your personal data with?

This section details who we may share your data with, this includes routine sharing as well as others who may have access to your data in limited and specific circumstances.

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

Who we may share data with varies by location and the specific circumstances, the main groups are listed in the table below:

Where	Who
Internal to NCC Group	Direct and indirect **line managers**, **HR professionals**, and **colleagues** related to the job role in question, where this is relevant to directly support the recruitment process, such as information shared for shortlisting.
	Other **members of NCC Group** to run global processes and to assist with workforce planning.
Externally to third parties	**Suppliers** to NCC Group where your personal data is required on a regular basis to provide the services, for example, our recruitment and HR systems.
	Providers of supporting systems that enable colleagues to work, such as office software, communications or conference platforms.
	Providers of software and systems for IT services, including security monitoring, such as endpoint protection, and hosting.
	Providers that **support** our **buildings**, **reception services**, **landlords** or **office maintenance** who support physical locations and may be based in or access one of our buildings.
	Providers who carry out **agreed processes** for NCC Group based on need, including screening providers, external search and assessment partners, external auditors and lawyers as relevant to your location and the job role in question.
	External auditors, **tax** or **other authorities**, **regulators** or **professional advisors** when this is relevant and required.

Any data disclosed to a third party will be processed only in accordance with NCC Group's instructions and to the extent necessary to deliver the service requested.

Some third parties to whom we may provide personal data, for instance auditors, professional advisers, or regulators, are independent controllers in their own right, and you should refer to their own privacy notices and policies in respect of how they use your personal data.

We may also be required to disclose your personal data to third parties in response to orders or requests from a court, regulators, government agencies, parties to a legal proceeding or public authorities, or to comply with regulatory requirements or as part of a dialogue with a regulator.

Your personal data may also be disclosed in connection with the consideration, negotiation or completion of a corporate transaction or restructuring of the business or assets of any part of NCC Group.

Please contact us if you have any questions regarding recipients of your personal data or would like more detail than is set out in this notice.

Back to top

Overseas transfers

NCC Group is a global business and therefore may need to transfer, or store, the data we process about you in a country outside of your jurisdiction. It may also be processed by colleagues or our suppliers operating outside your jurisdiction.

Transfers from the EU / UK / or the wider European Economic Area
We need to have legal grounds to transfer your data outside of the EU / UK. We currently base our legal transfers on the adequacy decisions of the EU Commissioner or the UK Information Commissioner's Office (ICO) or the Standard Contractual Clauses for transfers.

Adequacy decision
Some countries have been assessed as being 'adequate,' which means their legal system offers a level of protection for personal data which is comparable to the protection under the GDPR.

Standard Contractual Clauses (incorporated by our Intra Group Agreement)
Where the country or mechanism hasn't been assessed as adequate, we put into place an appropriate safeguard, or transfer mechanism, to protect personal data.

The method we use most frequently is Standard Contractual Clauses (SCCs). The European Commission and the ICO have recognised SCCs as offering adequate safeguards to protect your rights and we'll use these where required ensuring adequate protection for your information.
We have an Intra Group Agreement in place, incorporating these SCCs, alongside Transfer Impact Assessments for applicable countries, to allow sharing of your personal data between NCC Group employing entities globally.

Transfers from other countries

If you're based in a country outside of the EU / UK, there may be local obligations with regards to the transfer of personal data to other countries.

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 and contact details for more information.
- Philippines – no legal restrictions, although the controller remains responsible and accountable for all data under our control, and we use contractual clauses to provide protection.
- Singapore – standard contractual clauses & binding corporate rules are approved mechanisms.
- US – no restrictions around overseas transfers in the US although NCC Group will put into place safeguards.

For our service providers, we put into place contractual terms, including the SCCs, and make checks of their control environments to ensure that your data is treated compliantly, securely and in accordance with this privacy policy.

Back to top

How long do we keep your personal data Information for?

If you are successful and accept the role the personal data collected will become part of your employee file and will be retained in accordance with our retention schedule.
Otherwise we will retain your personal data for six months in all jurisdictions except for the Netherlands, which is set at four weeks, unless you provide us with consent to keep it for longer in to receive information on future opportunities.

If you become an employee we will retain your personal data in accordance with our Information Retention schedule, which is available on request to dataprotection@nccgroup.com.

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.

Back to top

Automated decisions and profiling

Automated decisions are where a computer makes a decision about you without a person being involved. We don't make any automated decisions about you.

For some roles we conduct limited profiling based on the result of psychometric tests you complete as part of our recruitment process to determine which questions you will be asked at the interview stage. This is sometimes used to determine what additional training may be relevant to you during the course of your future employment. This is carried out by specifically trained individuals who manually review any recommendations. You will be given more information prior to this processing taking place if this applies to you.

Back to top

Your rights under the GDPR

You have rights relating to the processing of your data under the GDPR which you can exercise free of charge, the global Data Protection & Governance Team will assess your request based on our ability to provide for your rights under GDPR, regardless of whether you are based in the EU or UK or not. Additional rights under local legislation are listed at the end of this document.

Access to your data - You have the right to ask for a copy of your personal 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 erasure - 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.

Data portability - In certain circumstances you have the right to ask us to provide your personal data in a structured, commonly used and machine-readable format, so that you can transmit the personal data to another 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.

Under the GDPR, organizations must respond to data subject requests—such as access, rectification, or erasure—without undue delay and within one month of receiving the request. This period may be extended by two further months for complex or numerous requests, but the data subject must be informed of the extension and the reasons for it within the initial one-month period.

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.

Back to top

Changes to this Privacy Notice

Any changes we may make to the Candidate Privacy Notice in the future will be added to this document and, where appropriate, notified to you by email. Please check back frequently to see any updates or changes.

Back to top

Contact details

Our Data Protection Officer can be contacted using the following email address: dataprotection@nccgroup.com, by phone on +44 7464 53 55 14 or alternatively by writing to XYZ Building, 2 Hardman Boulevard, Spinningfields, Manchester, M3 3AQ.

Questions, comments and requests regarding the Candidate 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 supervisory authorities;

UK	Information Commissioner's Office (ICO)	0303 123 1113 https://ico.org.uk/concerns/
European Union	Contact the supervisory authority in your location by consulting the list here	
Australia	Office of the Australian Information Commissioner	1300 363 992
Canada	Information Commissioner of Canada	1 800 267 0441 (option 9)
Singapore	Personal Data Protection Commission	+65 6377 3131
Philippines	National Privacy Commission (NPC)	+632 5322 1322 info@privacy.gov.ph
United States	Contact the Attorney General within your State – information on who your Attorney General is can be found here.	

Back to top

Special category personal data by country

Country	Racial or Ethnic Origin	Political, Religious, or Similar Beliefs and Opinions	Trade Union Membership	Physical or Mental Health	Sexual Life or Orientation	Genetic or Biometric Data	Additional categories of sensitive data:
Australia	X	X	X	X	X	X	
Canada (Federal)	X	X	Maybe	X	X	X	Information that may not be sensitive in one context, such as a name or email address, may become sensitive when connected to services that may reveal a user's personal activities and preferences. Other generally sensitive categories include: · Income-related information. · Credit history. · Information affecting an individual's reputation.
EU Member States and EEA Countries	X	X	X	X	X	X	Netherlands: information related to criminal convictions, financial data, legal identifier (BSN)
Philippines	X	X		X	X	X (genetic)	Marital status. Age. Education. Individualized information issued by government agencies, like Social Security numbers, previous or current health records, licenses (including grants, denials, suspensions, or revocations), and tax returns. Information that an executive order or Act of Congress declares classified.
Singapore	X	X	X	X	X	X	There is no separate definition of sensitive personal information, however, counts what a reasonable person would consider appropriate under the circumstances standard with advisory guidelines.
UK	X	X	X	X	X	X	Criminal records data
US (federal level)	X	X	X	X	X	X	Financial sector non-public personal information (Gramm-Leach-Bliley Act (GLBA)). Children's online personal information (Children's Online Privacy Protection Act of 1998 (COPPA)). Credit information consumer reports (Fair Credit Reporting Act (FCRA)). Social security numbers.

Other country specific information

Netherlands

The GDPR differentiates between personal data and special categories of personal data, as explained under "What kinds of information do we collect about you?". Under the Dutch jurisdiction, additional categories of **sensitive** personal data apply.

Sensitive personal data: financial data, legal identifier (BSN) and crime-related information

This includes specific categories of information that require extra protection under the GDPR due to their potential to impact an individual's privacy and security:

1. **Financial Data**: Information related to an individual's financial situation, such as bank account details, credit histories, or salary information. This data is sensitive as it can reveal a person's economic status and is protected to prevent identity theft or financial fraud and require extra care in the Netherlands.
2. **Legal Identifier (BSN)**: The Dutch citizen service number "**Burgerservicenummer" (BSN)** is a unique identification number assigned to every resident in the Netherlands. Processing is only allowed when legally required. It is used for a wide range of official and legal purposes, such as tax and social security administration. The BSN is highly sensitive, as it can be used to identify individuals in various databases, making it critical to protect it against unauthorized access.
3. **Crime-Related Information**: This includes data related to an individual's criminal history or involvement in criminal proceedings. Such data is classified as sensitive due to its potential to cause harm to an individual's reputation and privacy. Processing of crime-related information is only permitted under strict conditions, such as when required by law or for specific legal purposes (e.g., background checks for certain roles).

What does this mean for colleague's special/sensitive personal data processing in the Netherlands?

In practice, this brings the following additional protection:

Diversity information is not required for candidates in the Netherlands

In the Netherlands, the processing of diversity information, such as data on gender, ethnicity, age, or disability, is subject to strict regulations under the GDPR and Dutch anti-discrimination laws. Employers may collect and process this data to promote diversity and inclusion within the workplace, to comply with equal treatment regulations, or for specific reporting purposes, such as monitoring the effectiveness of diversity policies.
However, as this type of data is considered sensitive, explicit consent is generally required for its collection and processing. In some cases, such as when required for compliance with legal obligations or for statistical analysis in an anonymized format, the processing may occur without explicit consent. Employers must ensure that diversity information is kept confidential, processed securely, and used only for the intended purposes. Candidates have the right to request access to their diversity data, and any processing must comply with privacy rights and non-discrimination principles.
NCC Group does not require candidates in the Netherlands to share any diversity information.

Screening information

One of our entities in the Netherlands, Fox-IT, has a permit under the Private Security Organizations and Detective Agencies Act (or in Dutch: Wpbr) (link), and permission must be obtained from the chief of police for the candidates the company wants to employ (Article 7(2) of the Wpbr). Additionally, new Fox-IT employees are being screened by a private investigation bureau. Any criminal record checks must be performed via **Justis** (VOG) or a Wpbr-licensed screening bureau. For more information on the Fox-IT screening policy, please speak to your Talent Acquisition Partner.

Competent Supervisory Authority in the Netherlands

For candidates applying to Dutch entities, the Autoriteit Persoonsgegevens is the competent supervisory authority.

Autoriteit Persoonsgegevens
Hoge Nieuwstraat 8
P.O. Box 93374
2509 AJ Den Haag/The Hague
Tel. +31 70 888 8500
Fax +31 70 888 8501
Website: https://autoriteitpersoonsgegevens.nl/
Member: Mr Aleid Wolfsen - Chairman of the Autoriteit Persoonsgegevens

Philippines

In the Philippines the Privacy Act 2012 provides an additional right to compensation in respect of data subject's rights and the right to lodge a complaint with the National Privacy Commission.

United States

In the US identity checks are required on your first day of work and we attest to this using an I-9 form.

Colleagues will be asked to provide information on the veteran status to ensure that NCC Group complies with the Vietnam Era Veterans' Readjustment Assistance Act of 1974 (and as amended) which provides additional rights for protected veterans.

Colleagues that are California residents have rights under the California Consumer Privacy Act 2018 (CCPA). This includes the right to not have personal data sold or disclosed for valuable consideration between a business and a third party. This right excludes mergers and acquisitions.

United Kingdom

In the UK, we request identity checks when we want to make an offer as we need to see these before we can proceed with an offer. We also start the screening process at the point we issue an offer of employment

Canada

In Canada, screening providers aren't used so the process involves you obtaining a criminal record check yourself from the Royal Canadian Mounted Police.

Control information

Title	Candidate Privacy Notice
Version number	2.0
Date of issue	17 July 2025
Document owner	Group General Counsel
Quality approval	Data Protection and Governance Officer
Classification	General

Version history

Version	Date	Description of change
1.4	17/02/2022	General updates
1.5	22/06/2023	Amended due to introduction of diversity and data inclusion collection and more general updates following overall review.
1.6	26/10/2023	Addition of new entity and references to Philippine law, update of regulator information and internal contact details. Removed a reference to colleagues being able to sign up with benefits' provider whenever suits them best. Removed reference to ShareSave Privacy Policy.
2.0	17 July 2025	Overall review, updated branding, reformatting for clarity, and rewrite of key areas, incorporating feedback from the Works Council.