

GDPR Privacy Notice for Candidates

1. Purpose and Scope

The Rank Group Plc and its subsidiaries (“The Rank Group Plc” or “the Company”) is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you, in accordance with all data protection legislation, including the General Data Protection Regulation (GDPR). You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee worker or contractor). It applies to all prospective employees, workers and contractors from 25 May 2018.

The Rank Group Plc is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about data subjects. Prospective employees, workers and contractors are data subjects. We are required under data protection legislation to notify you of the information contained in this privacy notice.

The Rank Group Plc’s Data Protection Officer (“DPO”) is contactable via information.centre@rank.com. This is an email address manned confidentially by several employees who will escalate any queries to the DPO holding office from time to time. The DPO monitors internal compliance, informs and advises on the Company’s data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority, the Information Commissioner’s Office (“ICO”). If you have any questions about the application or interpretation of this candidate privacy notice please contact the Data Protection Officer (“DPO”) via information.centre@rank.com. You also have the right to make a complaint, at any time, to the ICO.

This notice applies to prospective employees, workers and contractors. It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical. Where prospective employees, workers and contractors are working overseas, local data protection laws and local policies may also apply. Should you become an employee, worker or contractor for the Company, the GDPR privacy notice for employees, workers and contractors in force from time to time will apply to you.

2. Data Protection Principles

The GDPR sets out principles with which data controllers must comply when processing personal data (Article 5 of the GDPR). This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

3. The kind of information we hold about you

We hold personal data and sensitive personal data.

3.1 Personal Data

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We will collect, store, and use the following categories of personal information about you:

- The information you have provided to us in your curriculum vitae and covering letter.

- The information you have provided on our application form, including name, title, address, telephone number, personal email address, date of birth, gender, employment history, qualifications and personal interests.
- Any information that you provide to us during an interview.
- Any other information that you provide as part of an application process such as test results.
- Information relating to your identity and right to work in accordance with The Rank Group Plc Employee Eligibility Policy.
- Information in social media accounts which are publicly accessible.

3.2 Sensitive personal data

There are special categories of more sensitive personal data which require a higher level of protection under the GDPR. Details about how we will process that data are set out in section 8. The sensitive personal data that we may collect store and use from time to time are:

- Information about your race or ethnicity, religious beliefs, sexual orientation philosophical beliefs and political opinions.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records.
- Biometric data.
- Information about criminal convictions and offences.

4. How Is Your Personal Information Collected?

We collect personal information about prospective employees, workers and contactors through the application and recruitment process, either directly from candidates and sometimes from

- Employment agencies
- Background check providers
- Credit reference agencies
- The Disclosure and Barring Service
- Your named referees
- Public sources including publicly accessible social media sites
- Government agencies
- Medical professionals
- Industry related bodies, such as the gaming commission.

5. How we will use information about you

We will only use your personal information when the law allows us to and we will sometimes ask for your explicit consent for a specific purpose. However, most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

We need to process the categories of information listed at paragraph 3 primarily to pursue our legitimate interests in deciding whether to appoint you to a role. We also need to process the categories of information to enable us to enter into a contract with you if you are appointed and to enable us to comply with legal obligations. The situations in which we will process your personal information are listed below: -

- Making a decision about your recruitment or appointment
- Assessing your skills, qualifications and suitability to work
- carrying out background and reference checks

- communicating with you about the recruitment process
- Keeping records relating to the hiring process
- Complying with legal or regulatory requirements
- Ensuring meaningful equal opportunity monitoring and reporting
- Checking whether you are legally entitled to work in the UK

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6. Failure to provide information

If you fail to provide certain information when requested, we may not be able to process your application successfully or we may be prevented from complying with our legal obligations.

7. Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

8. How we use sensitive personal data

We need to have further justification for collecting, storing and using sensitive personal data. We have in place an appropriate policy document and improving safeguards which we are required by law to maintain when processing such data. We may process sensitive personal data from time to time in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information 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 sensitive personal data in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- We will use information about criminal convictions and offences to determine your suitability for a role.
- We will use biometric CCTV data as set out in section 9.

Do we need your consent?

We do not need your consent if we use sensitive personal data in accordance with this privacy notice to carry out our legal obligations or exercise specific rights in the field of employment law but in limited circumstances, we may approach you for your written consent. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us. Where consent is not given the Company may sometimes need to make a decision without all relevant information.

9. CCTV and other cameras

There are closed circuit television cameras (“CCTV”) and other cameras in operation within the Company’s Casinos, Bingo Clubs and other premises, which, depending on the respective country and applicable laws, may be used for the following purposes:-

- To prevent and detect crime.
- To protect the health and safety of customers and colleagues.
- To manage and protect the Company’s property and the property of customers, colleagues and others.
- As part of the broadcast of certain games across the Company’s locations and locations of other providers of such games.
- For training purposes.
- As part of an investigation, disciplinary and/or grievance process.

CCTV images and footage are biometric data and will be processed in accordance with section 8.

10. Information about criminal convictions

We envisage that we may hold information about criminal convictions and offences.

We may only use information relating to criminal convictions and offences where the law allows us to do so; presently this is allowed through voluntary disclosure or official criminal records checks through the Disclosure and Barring Service (“DBS”). This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with this privacy notice and the Data Protection Policy.

Less commonly, we may use information relating to criminal convictions and offences where it is necessary 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. We may also process such information in the course of legitimate business activities with the appropriate safeguards.

We will only collect information about criminal convictions and offences 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. We will use information about criminal convictions and offences in order to determine your suitability for working for us before you join the Company.

We are allowed to use your personal information in this way to carry out our obligations. We have in place an appropriate policy and improving safeguards which we are required by law to maintain when processing such data.

11. Automated decision-making

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.

12. Data sharing

12.1 Sharing with third parties

It is unlikely but possible that we may have to share your data with third parties, including third-party service providers and other entities in The Rank Group Plc. If we do, you can expect a similar degree of protection in respect of your personal information. We require third parties to respect the security of your data and to treat it in accordance with the law. All our third-party service providers and

entities in The Rank Group Plc are required to take appropriate security measures to protect your personal information in line with our policies.

We will share your personal information with third parties where required by law, where it is necessary to administer the recruitment process with you or where we have another legitimate interest in doing so.

12.2 Transfer outside of the EU

It is unlikely but possible that we may transfer your personal data outside the EU and Alderney (an EU approved jurisdiction) to Guoco Management Company Limited (“GMCL”) a company registered in Hong Kong. GMCL is a company within the group of companies owned by the majority shareholder of The Rank Group Plc, Guoco Group Limited (“Guoco”) which is a company listed in Hong Kong.

We may also transfer your personal data outside the EU to HL Management Co Sdn Bhd (“HL”), a company listed in Malaysia and the ultimate parent company of Guoco.

The purpose of any transfer to GMCL and/or HL is for group human resource planning and administration purposes to help achieve efficiency, fairness and equality across the group.

There is no adequacy decision by the European Commission in respect of Hong Kong and Malaysia which means that these countries are not automatically deemed to provide an adequate level of protection for your personal information.

However, to ensure that your personal information does receive an adequate level of protection we have put in place the following appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection: We have a data processing agreement in place between The Rank Group Plc with both GMCL and HL which require them to treat your personal data in accordance with the GDPR. If you require further information you can request it from the DPO at information.centre@rank.com.

It is unlikely but possible that your personal data may also be transferred outside the EU and Alderney by our third-party service providers. Such entities are required to take appropriate security measures to protect your personal information in line with our policies.

13. Data security

We have put in place appropriate security measures and improving safeguards to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the DPO at information.centre@rank.com.

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.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

14. Data retention

We will only retain your personal information 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. Details of retention periods for different aspects of your personal information are available in The Rank Group Plc policy that refers to data retention in force from time to time. 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.

In some circumstances, we may anonymise your personal information 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 a prospective employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with The Rank Group Plc policy that refers to data retention from time to time.

15. Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during the recruitment process.

16. Your rights and obligations

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.
- **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 refer to The Rank Group Plc policy that refers to Data Subject Access Requests in force from time to time.

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.

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 information is not disclosed to any person who has no right to receive it.

17. Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

18. Data protection officer

We have appointed a DPO to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

19. Responsibility for and 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 information.

The Human Resources Department in conjunction with the DPO has the responsibility for ensuring the maintenance, regular review and updating of this privacy notice. Revisions, amendments or alterations can only be implemented following consideration by the GHRD and/or the DPO.