Delaware North Privacy Notice – Job Applicants

This Privacy Notice sets out details about the personal data that we, Delaware North Companies (UK) Services Ltd ("Delaware North"), may collect and process about you.

This Privacy Notice is non-contractual, regularly reviewed and may be amended by us from time to time.

Types of data we may process

Recruitment Stage

We may process the following information at the recruitment stage:

- Personal contact details including name, address and email.
- Information collected during the recruitment process such as your CV/application (including details of previous work experience, education and references) and answers to any interview/recruitment questions relevant to the role you applied for.
- Psychometric testing results, where such tests are used as part of any application process (see "Automated Decision Making" below).
- Equal opportunities information. This is not mandatory and is not made available to anyone outside of the recruitment team (including hiring managers and HR) save in an anonymised format so as not to identify you.
- Recruitment Agencies – we may collect your personal details, details of your application and details of your experience and qualifications from the recruitment agency you applied via.
- Basic Disclosure checks. This will reveal details of any unspent criminal convictions and is processed by the Disclosure and Barring Service. These checks are required to safeguard staff and members of the public at our protected venues and for some venues is a security requirement to work on site. Further details can be found in our Safeguarding Policy.
- For some roles, where required by law, an Enhanced Disclosure may be required. Further details can be found in our Safeguarding Policy.
- Global Watch List checks. These are recommended by the National Counter Terrorism Security Office (NaCTSO) and is a collection of caution lists from all major sanctioning bodies, law enforcement agencies and financial regulators worldwide. It is used to reveal whether individuals are on a sanctions list or are a politically exposed person. It is a crucial tool in ensuring all staff on site are not affiliated with any terrorist organisation and/or pose a risk to the public and other members of staff. Further details can be found in our Safeguarding Policy.

With the exception of the equal opportunities information and Basic Disclosure and Global Watch List checks, you are obliged to provide this personal data to us as it is necessary for us to explore potentially entering into a contract with you. The equal opportunities form is not mandatory and there are no consequences if you fail to provide it. However, if you do not submit

your Basic Disclosure information or information for the Global Watch List checks, you may be unable to work at some of our venues, in line with the security protocols at the venues.

If you fail to provide any of the data you are obliged to provide, we may be unable to process your application and, if appropriate, offer you employment or variable work.

Conditional Offer/Shortlisted

We may process the following information after you have been shortlisted and/or as part of a conditional job offer:

- Proof of your identity (such as driving licence) and any relevant right to work checks;
- Proof of your qualifications – unless you are specifically notified that we will accept a copy of your qualifications which we can verify, you will be asked to attend our office with original documents and we will take copies;
- We will contact your referees (with express consent), using the details you provide in your application, directly to obtain references.

The above is usually part of a conditional offer of employment or variable work and therefore you are obliged to provide this as it is necessary to enable us to enter into a contract with you. Right to work checks are a statutory requirement which you are obliged to provide. A failure to provide this may result in us being unable to offer you employment or variable work.

The purposes of processing

- For recruitment purposes i.e. to ensure you are suitable for the role being advertised and so we can contact you about this role;
- To comply with legal obligations including right to work checks;
- To seek professional advice advice/defend claims arising from the recruitment process;
- In line with the security requirements at some of our venues, to safeguard our staff and members of the public.
- In relation to the equal opportunities form, to monitor equality in recruitment practices.

Please note that if we intend to further process your personal data for a purpose other than that for which it was collected, we shall provide you with information on this other purpose and all other information as set out in this notice.

Sharing your data

Your data will be shared internally with the recruitment team which consists of HR, the interviewing staff and managers at Delaware North, as relevant, and their support staff and subordinates where appropriate.

If your role falls into a Joint Venture between Delaware North and a third party, the information may be shared between us and the HR team and managers of the Joint Venture to enable the Joint Venture to make a decision about the role you have applied for.

Transferring information outside the European Economic Area (EEA)

We may transfer the personal information we collect about you with other Delaware North Companies, including Delaware North for America, which is based in New York State and in other locations outside the EEA, in order to perform our contract with you and for the purposes of Delaware North for America's regular and periodic audits on its subsidiary companies

(including Delaware North Companies (UK) Services Limited and any of its subsidiaries). These audits are necessary for the business and for the Delaware North for America to analyse our financial and business performance, as well as the adequacy of the systems and controls of Delaware North Companies (UK) Services UK Limited and the Delaware North group of companies as a whole.

There is an adequacy decision by the European Commission in respect of this country through the EU-US Privacy Shield ("**Privacy Shield**"). This means that the country to which we transfer your data is deemed to provide an adequate level of protection for your personal information as long as any transfer meets the safeguards of the Privacy Shield.

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:

- Only personal data that is necessary for the purposes of the audit or otherwise in the performance of our contract with you will be disclosed.

- Such data will be limited to those individuals for whom the audit or other purpose is carried out and will be on a need to know basis.

- Such information will be kept confidential by the individuals conducting the audit or other purpose.

- Any personal data to be disclosed shall (if appropriate) be redacted, and in any event retained for no longer than is necessary for our (and our Group and Parent companies') compliance and due diligence obligations.

- Appropriate security measures will be taken when transferring the data.

How long we keep your data

In terms of retention periods, we will not keep your data for longer than is necessary. When deciding how long to hold your data we have regard to legal requirements (including any contractually agreed periods) and statutory limitation periods (under which it is prudent for us to retain records for longer periods).

Legal basis for processing

We process your personal data on the basis of consent (for example where we contact your referees, for equal opportunities and security check purposes) and/or because it is necessary for our legitimate interests, namely to ensure that you are qualified and suitable for the role you are applying for, to ensure we have a record of the recruitment process for the defence of legal claims and to comply with our security obligations.

We process details of your right to work checks in line with our legal requirement to do so.

Consent

Where we rely on consent to process your personal data, you have a right to withdraw your consent at any time. This will not affect the lawfulness of processing based on consent before its withdrawal.

You can withdraw your consent to our processing at any time by contacting the HR department on helpmeout@delawarenorth.com. Please specify the type of processing that you are withdrawing your consent to in your email.

Your rights

You have a number of rights in relation to the personal information that we process about you. You:

- Have the right to be informed about your data (as set out in this Privacy Notice);
- Can request access to your personal data;
- Can request that your personal data be rectified if it is inaccurate or incomplete;
- Can request that the processing of your personal data be restricted or erased in certain circumstances, for example, where the data is no longer necessary to meet its purpose;
- Can object to processing in certain circumstances, for example where this is based on legitimate interests or involves direct marketing;
- Can request to receive personal data that you have provided in a structured, commonly used and machine-readable format and to have this transmitted without hindrance where the data is processed on the basis of consent or performance of a contract;
- Can lodge a complaint with the Information Commissioner's Officer.

Automated Decision Making ("ADM")

ADM occurs when decisions are made about you by a computer or some other information analysing machine. Examples of this include the machine scanning of CVs, computer processed aptitude or personality tests and website profiling. There are circumstances when we use ADM during the recruitment process. If you feel you may have been subjected to ADM and wish to request human intervention or challenge the decision, please contact….
Where any psychometric testing is used as part of any application or for any ongoing development with us, any such profiles generated are reviewed by HR and/or your manager, as relevant, and the outcomes and any decisions resulting from such tests will not solely be based on ADM.

Contact details for Data Controller and enquiries

Delaware North Companies (UK) Services Ltd (registered in England and Wales with company no**. 05573788**) can be contacted at Capital Court; 30 Windsor Road, UB8 1AB Tel: 020 8453 5060**.**

If you have any enquiries regarding data protection or wish to exercise any of your rights, please do contact the HR department on helpmeout@delawarenorth.com.

POLICY EFFECTIVE FROM: September 2019