EMPLOYEE PRIVACY NOTICE

The organisation collects and processes personal data relating to its employees to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

WHAT INFORMATION DOES THE ORGANISATION COLLECT?

The organisation collects and processes a range of information about you. This includes:

- your name, address, and contact details, including email address and telephone number, date of birth and gender.
- the terms and conditions of your employment.
- details of your qualifications, skills, experience, and employment history, including start and end dates, with previous employers and with the organisation.
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover.
- details of your bank account and national/social insurance number.
- information about your marital status, next of kin, dependants, and emergency contacts.
- information about your nationality and entitlement to work in Gibraltar.
- information about your criminal record.
- details of your schedule (days of work and working hours) and attendance at work.
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave.
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence.
- information about medical or health conditions, including whether you have a disability for which the organisation needs to make reasonable adjustments.
- details of trade union membership
- equal opportunities monitoring information, which may include information about your ethnic origin, sexual orientation, health and religion or belief.

The organisation collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

The organisation seeks information from third parties with your consent only.

Data is stored in a range of different places, including in your personnel file, in the organisation's HR management systems and in other IT systems (including the organisation's email system).

WHY DOES THE ORGANISATION PROCESS PERSONAL DATA?

The organisation needs to process data to enter an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefits such as pension and Health and Life insurance entitlements.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in Gibraltar, to deduct tax, to comply with health and safety laws, to enable employees to take periods of leave to which they are entitled, and to consult with employee representatives if redundancies are proposed or a business transfer is to take place. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes.
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights.
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace.
- ensure employees are complying with relevant policies and procedures.
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes.
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled.
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled.

- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration.
- conduct employee engagement surveys.
- provide references on request for current or former employees.
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the organisation uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time by contacting policies@eyasgaming.com. Employees are entirely free to decide whether to provide such data and there are no consequences of failing to do so.

WHO HAS ACCESS TO DATA?

Your information will be shared internally, including HR and recruitment team (including payroll), your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

Your data may also be shared with employee representatives in the context of collective consultation on a redundancy or business sale. This would be limited to the information needed for the purposes of consultation, such as your name, contact details, role, and length of service.

The organisation shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks where necessary from the Disclosure and Barring Service. The organisation may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The organisation also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services.

The organisation will not transfer your data to countries outside the European Economic Area.

1. In terms of GDPR requirements post Brexit according to the GRA the situation will be as follows:
    a. for GDPR disclosure to entities within the UK there will be a specific agreement in place between the UK and Gibraltar. This is likely to mirror what is currently in place.
    b. for GDPR disclosure to entities within the EEA the rules will stay the same, therefore if you have to disclose HR information to Malta or Germany for example the usual EU rules and requirements will apply as before (which are the rules we have in place currently)
    c. for GDPR disclosure outside of the EEA and the UK the usual rules will apply and it will depend on the GDPR rules of that country as to whether it is deemed by the EU to have an adequacy decision in place. It is understood that this provision will remain

within Gibraltar law post Brexit. The GRA website has some extremely helpful information about Data Protection generally and about post Brexit requirements.

HOW DOES THE ORGANISATION PROTECT DATA?

The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

FOR HOW LONG DOES THE ORGANISATION KEEP DATA?

The organisation will hold your personal data for the duration of your employment. The periods for which your data will be held after the end of employment (subject to any additional periods confirmed to you in writing) are

Example of Employee Data	**Retention period**
Notes from interviews unsuccessful candidates	6 months
Payslips and records relating to wages	Minimum 3 years maximum 6 years
Contractual information (working hours address, roles and responsibilities)	Minimum 3 years maximum 6 years
Termination records; redundancies	6 years
Records relating to Parental leave	6 years
Tax and SI records	Minimum 3 years –maximum 6 years
Records relating to workplace accidents	10 years (or as required)
Pension or Health Insurance records	Maximum 12 years
Employment permits/visa information	6 years or duration of employment.

YOUR RIGHTS

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request.
- require the organisation to change incorrect or incomplete data.
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing.

- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.
- If you would like to exercise any of these rights, please contact policies@eyasgaming.com

You can also make a subject access request by contacting the above address

If you believe that the organisation has not complied with your data protection rights, you can complain to the Gibraltar Regulatory Authority (GRA)

What if you do not provide personal data?

You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in Gibraltar and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.