Candidate Privacy Notice

Version: 1.0

Date: Nov 10, 2025.

1. WHAT IS THE PURPOSE OF THIS DOCUMENT?

1.1. This Candidate Privacy Notice (hereinafter, also referred to as "Notice") is applicable to candidates of Adjarabet whose personal information ("you", "your") is used within the recruitment process.

1.2. The purpose of this Notice is to describe how we collect and use personal information about you before, during and after the recruitment process. It also explains your rights regarding your personal information and how to exercise them.

1.3. It is important that you read this Notice, together with any other notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

1.4. This Policy is governed by and interpreted in accordance with the Laws of Georgia.

2. WHO WE ARE

2.1. For the purposes of this document, the following companies within the Adjarabet group may act as the employing entity depending on the role you are applying for:

• AB Georgia LLC (ID 405076304) – Legal Address: Chubinashvili Street N55, Chugureti district, Tbilisi, Georgia

• Adjarapay LLC (ID 404984978) – Legal Address: Chubinashvili Street N55, Chugureti district, Tbilisi, Georgia

• Advanced Systems LLC (ID 405425936) – Legal Address: Chubinashvili Street N55, Chugureti district, Tbilisi, Georgia

Hereinafter, the relevant entity (depending on your application) is referred to as "us", "we" or "Adjarabet."

2.2. For the purposes of this policy and in accordance with Georgian data protection legislation, Adjarabet acts as the "data controller" in relation to the Processing of your personal data. The data controller is responsible for deciding how personal information about you is processed.

3. HOW IS YOUR PERSONAL INFORMATION COLLECTED?

3.1. We collect information directly from you during your recruitment journey and sometimes we collect information about you from third parties (e.g. from an employment agency, talent lifecycle provider, previous employers and background check provider(s)). We may use information collected from publicly available sources, including social media sites such as LinkedIn, to identify, reach out and build a profile of candidates. We will also process information that you provide or generate when interacting with our recruitment platforms/websites.

3.2. If you have applied directly for a role on one of our **career websites** (which include https://apeople.ge/) you will be asked to provide your personal information which will be used to create a candidate profile on you. If you apply through other channels, a candidate profile will be created only if you are shortlisted. This information may be shared with third parties as required, which may include our talent lifecycle providers, online assessment, or background check provider, where we have legal requirements to

undertake such checks, or otherwise in accordance with applicable laws and internal policies [see more information below].

3.3. If you fail to provide certain information during the application process, when requested, we may not be able to continue with the application process (such as not being able to confirm your right to work in the country that you are applying to work in).

3.4. 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. We will always have a lawful basis under privacy laws to collect and process your data, see details below in section 5.

4. THE CATEGORIES OF INFORMATION WE HOLD ABOUT YOU

We may collect, store, and use the following categories of personal data about you (note that this list is comprehensive but not necessarily exhaustive):

Categories of Personal Data	**Types of Data**
Personal details	- Name, gender, nationality, date of birth, age, personal contact details (e.g. address, telephone or mobile number, e-mail), national ID number (usually at the final stage of the recruitment process), languages spoken.
Financial	- Remuneration information (including salary expectation).
Recruitment	- Skills and experience, qualifications, referrals, CV and application, interview and assessment data, right to work verification (including passport, visas or identity cards) information related to the outcome of your application, details of any offer made to you, relevant professional and educational qualifications, references, background and verification information (e.g. when shortlisted results of financial sanction check where carried out and permitted by applicable laws).
Training and development	- Data relating to training and development needs or training received, or assessments completed.
Sensitive	- Where permitted by law or provided voluntarily, special category data regarding race, health and ethnicity, also, criminal data relating to criminal convictions and offences.
Publicly available data	- Any personal information which is publicly available, such as LinkedIn profile information, social channels, or media & news outlets including phone, email, social websites links, skills, education history, job history that is available publicly.
Online	- Cookies: This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience.
Other	- Information linked to private activities. For example, where we may gather additional personal information, usually at the final stage of the recruitment process, about family relationships, occupation or otherwise.

	- Any other personal information which you choose to disclose to us during your recruitment whether verbally or in written form.

5. HOW AND WHY WE WILL USE PERSONAL INFORMATION ABOUT YOU

We will use your personal data for the following purposes and related lawful bases:

Purpose	**Purpose for Processing**	**Categories of Personal Data**	**Lawful Bases of Processing**
Recruitment	To enable us to make decisions regarding your suitability to work for us. To provide any appropriate adjustments or accommodations required in the recruitment process.	Personal details; Financial; Recruitment; Training and development; Sensitive; Publicly available data; Other.	a) Our statutory duties (including financial crime, wellbeing, health and safety regulations); b) To enter into a contract at your request; c) The processing of sensitive data is necessary because of the nature of employment obligations and relations, including for making decisions on employment and assessing the working capacity of the employee; d) Our legitimate interests in identifying and assessing potential candidates for open roles. Such as: - Managing Conflict of Interest; - Protecting company and customer property and assets – ensuring candidates entrusted with access to company systems or facilities can be relied upon; - Protecting our organization against risk of financial crimes such as money laundering, terrorism, and bribery; - Ensuring information security – safeguarding confidential data and preventing fraud or misuse; - Protecting health and safety of other employees and customers – e.g., by screening for past conduct relevant to workplace safety; - Protecting company reputation and business integrity – avoiding hiring individuals who may pose compliance or other legitimate risks; - Compliance with group minimum standards and policies;

			- defending possible future legal claims; e) Data is publicly available.
Website management and Cookies	To ensure that our career websites work properly for your device. Identify errors on the site. To understand how people, reach our site. To assess the effectiveness of our career websites site and their content.	Online	a) Our legitimate interest to run effective career websites; b) Your consent, where applicable.
Pre-employment verification and background screening	To undertake appropriate pre-employment screening (including Financial Crime (such as complete adverse media, PEPs and sanction) screening). Including to enable us to make decisions regarding your suitability to work for Adjarabet.	Personal details; Recruitment; Training and development; Sensitive; Publicly available data; Other.	a) Our statutory duties (including financial crime, wellbeing, health and safety regulations); b) To enter into a contract at your request; c) The processing of sensitive data is necessary because of the nature of employment obligations and relations, including for making decisions on employment and assessing the working capacity of the employee; d) Our legitimate interests of ensuring suitable candidates are placed in roles. Such as: - Managing Conflict of Interest; - Protecting company and customer property and assets – ensuring candidates entrusted with access to company systems or facilities can be relied upon; - Protecting our organization against risk of financial crimes such as money laundering, terrorism, and bribery; - Ensuring information security – safeguarding confidential data and preventing fraud or misuse; - Protecting health and safety of other employees and customers – e.g., by screening for past conduct relevant to workplace safety; - Protecting company reputation and business integrity – avoiding hiring

			individuals who may pose compliance or other legitimate risks; - Compliance with group minimum standards and policies; - defending possible future legal claims; e) Data is publicly available.
Job opportunities & Talent community communications	To contact you in relation to job opportunities which we consider may be of interest to you. To send you recruitment related communications.	Personal details; Financial; Recruitment; Training and development; Publicly available data; Other.	a) To enter into a contract at your request; b) Our legitimate interest to identify suitable candidates for roles; c) Your consent, where applicable.

6. DATA SHARING

6.1. In addition to the purposes involving the processing of your personal information listed above, we may also disclose your personal information to third-party service providers and other entities in Flutter Entertainment PLC (the) Group ('Flutter').

6.2. All our third-party service providers and other relevant entities in Flutter are required to have appropriate technical and organizational measures, including security measures to protect your personal information, e.g. within systems to have restricted access to your data. This means only those who need to use it, can access it.

6.3. As part of a global organization, your personal information may be accessed by colleagues across Flutter where we have a legitimate interest, for the following purposes:

- due to contractual necessity to meet our obligations in your contract of employment where those obligations might be fulfilled by a member of Flutter other than your employer entity.
- Human Resource operations including access by brands in Flutter to our Flutter talent community.
- Providing global support and services in Legal, Compliance & Risk.
- Meeting our regulatory obligations.
- Reporting and group oversight.
- As part of our regular reporting activities on company performance, in the context of a business reorganization or group restructuring exercise, for system maintenance support and hosting of data.
- For the continuity of recruitment in the event of a merger or takeover.

6.4. Depending on the circumstances, third parties, or legal entities in Flutter may be considered Data Processors or Controllers of your personal information.

6.5. We may also share your personal information with third-party service providers, including contractors and designated agents. These third parties may perform certain functions on our behalf, such as:

- Supporting recruitment-related activities;

- Creating and maintaining candidate profiles;
- Assessing and verifying eligibility to work in the relevant jurisdiction, where applicable;
- Conducting background screening checks; and
- Ensuring compliance with legal and regulatory obligations or supporting the defense of legal claims.

6.6. We may also disclose your personal information in the following circumstances:

- When required by applicable law or regulation (disclosure to a governmental, regulatory or enforcement authority);
- In order to defend ourselves legally and/or in relation to legal proceedings; and
- Whilst negotiating a takeover, purchase, merger or divestiture and pursuant to the same.

6.7. From time to time personal information we collect about you will be transferred outside the Georgia to other Flutter entities or third parties in accordance with our lawful basis for processing that information.

We will ensure that the appropriate measures to protect your personal information are in place for such transfers, including;

- An intra-group data protection agreement which includes required contractual clauses, as well as security contractual clauses, applicable to cross border transfers of personal information in Flutter, as required by law;
- Where applicable, relevant contractual clauses in our contracts as required by law; and
- Where applicable, additional safeguards to ensure the protection of your personal information in all destination jurisdictions.

7. DATA SECURITY

We take appropriate security, technical and organizational measures to ensure that your personal information is kept secure and to prevent the theft, loss, or unauthorized access to your personal information. We restrict access to those who need to use and view it. If you believe your personal information has been leaked or breached, please contact us. The matter will be investigated immediately.

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.

8. DATA RETENTION

8.1. We endeavour to ensure that personal information is kept as up to date as possible, and that irrelevant or excessive data is deleted or made anonymous as soon as reasonably practicable. As a part of talent community, we generally retain your personal information for 2 years.

8.2. Where we process data based on your consent, you have the right to ask for your data to be deleted at any time, see section 9 for further details.

8.3. Where your recruitment process is successful and you become an employee of Adjarabet, your information will be processed and retained as described in our Staff Privacy Notice (which will be available to you upon joining).

9. YOUR RIGHTS

9.1. Under certain circumstances, by law you have the following rights in connection with your personal information:

- Request information about the collection and processing of your personal data.
- Request access to your personal data as well as the transfer of their copies.
- Request termination of the processing, erasure or destruction of your personal information.
- Request blocking, modification, correction, update, completion, addition, transfer of your data if they are incomplete, inaccurate, outdated, or if their collection and processing were conducted unlawfully.
- Right to portability. This right allows you to obtain your personal data in a structured and transmittable format.
- Withdraw consent at any time and without explanation.

Please note that in certain circumstances envisaged by the legislation, if the processing serves our and/or a third-party legitimate interests and/or is necessary for the provision of services, and/or is required for the data controller to fulfill obligations imposed by applicable legislation, Adjarabet may refuse to provide the request.

9.2. Right to Complain

If you have any complaints, you have the right to contact Personal Data Protection Service. However, we ask that you contact us at compliance@adjarabet.com; compliance@adjarapay.com; or compliance@advancedsystems.ge in the first instance to allow us the opportunity to address your concerns.

10. RIGHT TO WITHDRAW CONSENT

In the circumstances where you have provided your consent to us to use your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. You can do this by contacting us at hr@adjarabet.com.

11. DATA PROTECTION OFFICER

If you have any questions about this Notice or how we handle your personal information, please contact our Data Protection Officer via email at:

- compliance@adjarabet.com (AB Georgia LLC)
- compliance@adjarapay.com (Adjarapay LLC)
- compliance@advancedsystems.ge (Advanced Systems LLC)

12. CHANGES TO THIS NOTICE

We reserve the right to update this Notice at any time. Updated notices will be published on our career website along with update date.