



Privacy Notice

1. Introduction

This Privacy Notice outlines our practices concerning the collection, use, and safeguarding of your personal data.

This notice applies to all Job Applicants. It is designed to meet our duties of transparency under the privacy legislation and to ensure you understand our approach to your personal data.

Please read this notice carefully to understand our practices regarding your personal data and how we will treat it. If you have any questions or concerns about this notice or your data protection rights, our contact details are provided at the end of this document for your convenience.

2. Who are we?

SuprPlay Ltd, a Maltese company with company registration number C-74595, is the personal data controller responsible for the processing of your personal data. This policy describes our processing of personal data. SuprPlay Ltd. processes your personal data in compliance with the EU General Data Protection Legislation (the "GDPR"), (Regulation 2016/679) and the Maltese Data Protection Act (Chapter 586 of the Laws of Malta) as well as the various subsidiary legislation issued under the same.

SuprPlay is part of the SuprNation Group ("SuprNation" or "SN"). We can be contacted at the following address: Palazzo Villa Rosa, Triq in-Nemes, Swieqi, Malta.

3. Collection of Personal Information

We collect personal information about you during the recruitment process directly from you and, where applicable, from third parties such as recruitment agencies or background check providers. This information includes but is not limited to your name, contact details, resume, employment history, educational background, and references.

We may also collect certain demographic data that qualifies as sensitive personal data, such as race, ethnicity, sexual orientation, and disability to help us understand the diversity of our workforce. This information is on a voluntary consensual basis, and you are not required to provide this information, unless it is necessary for us to collect such information to comply with our legal obligations.

4. How we process your personal data

Your personal information will be used to:

- Assess your suitability for the role you have applied for.
- Communicate with you about the recruitment process.
- Carry out background and reference checks, where applicable.
- Comply with legal or regulatory requirements.

5. What is the legal basis for processing your personal data?

SuprPlay Ltd

Palazzo Villa Rosa, Triq in-Nemes, Swieqi SWQ 3302, Malta – Europe

VAT No: MT 2424-0231 C-74595

The lawful basis for processing your personal information for these purposes includes:

- Consent: You have given clear consent for us to process your personal data for the purpose of recruitment process.
- Contractual necessity: The processing is necessary in order to take steps at your request before entering into a contract.
- Legal obligation: The processing is necessary for compliance with a legal obligation to which we are subject.
- Legitimate interests: The processing is necessary for our legitimate interests or the legitimate interests of a third party, provided those interests are not overridden by your rights and interests. These interests include managing our recruitment process, verifying your information, and making hiring decisions.

6. Sharing of Your Personal Information

We may share your personal information with third parties involved in the recruitment process, including recruitment agencies, background check providers, and our affiliates. Any third-party service providers we use are required to take appropriate security measures to protect your personal information.

7. How long we keep your personal data

We will retain your personal information for as long as necessary to fulfill the purposes identified in clause 5, including for the purposes of satisfying any legal, accounting, or reporting requirements.

If unsuccessful, we will delete your data 6 months after the recruitment process has been finalized, unless you give us your permission to keep it for the purposes of any future openings or it is necessary to retain the data to defend potential legal claims.

8. Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data:

- The right to request a copy of your personal data which Company holds about you unless there are legally binding restrictions forbidding us to share all the information we process,
- The right to request that Company corrects any personal data if it is found to be inaccurate or out of date,
- The right to request your personal data is erased where it is no longer necessary for Company to retain such data (unless Company has a right to process data e.g. to defend its legal claims),
- The right to withdraw your consent to the processing at any time,
- The right to request that Company to provide you with your personal data and where possible, to transmit that data directly to another data controller
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing
- The right to object to the processing of personal data
- The right to lodge a complaint with the Information and Data Protection Commissioners Office

Generally, exercising your rights is free of charge. However, if your request is clearly unfounded, repetitive, or excessive a reasonable administrative fee may be charged. Company shall provide you with a response without

undue delay, and in any event within 1 month starting from the date that your identity is verified. Please note that verification of your identity is a security measure to ensure that personal data is not disclosed to any unauthorized person.

9. Transfer of data outside of the EU

Where personal data is intended to be transferred outside of the EU, the GDPR imposes restrictions to ensure the protection of individuals is not undermined by taking the necessary actions so that your privacy rights continue to be protected, as stated in this Job Applicant Data Privacy Notice and in accordance with Data Protection Legislation. Company will ensure that any transfers within the group companies provide for adequate safeguards as enforced by the Information and Data Protection Commissioners Office.

10. Further processing

If we wish to use your personal data for a new purpose, not covered by this Job Applicant Data Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

11. Data Security

Company takes information security seriously and strives to comply with our regulatory and legal obligations at all times. Any personal information collected will have appropriate safeguards applied in line with obligations arising out of Data Protection Legislation.

Your information is protected by controls designed to minimise loss or damage through accident, negligence or deliberate actions. This includes:

- Encryption: data is stored on a reputable cloud (Google and Dropbox) which encrypts data;
- Strong password requirements;
- Access restrictions: only a restricted number of person(s) within the Company have and will have access to your personal data;
- Keeping personal information up to date;
- Storing and destroying it securely;
- Data minimization: not collecting or retaining excessive amounts of data;
- Protecting personal data from loss, misuse, authorized access and disclosure;
- Ensuring that appropriate technical measures are in place to protect personal data.

12. How to make a complaint

Company will always strive to collect, use and safeguard your personal information in line with Data Protection Legislation. If you do not believe we have handled your information as set out in this Job Applicant Data Privacy Notice or in accordance with applicable Data Protection Legislation, please contact us immediately to put things right.

If you believe the matter is still unresolved you can make a complaint to [the Information and Data Protection Commissioners Office](#).