Human Resources Data Privacy Policy

NASPERS

1. INTRODUCTION

1.1. Naspers recognises privacy as an important value, and as an essential element of employee's trust. Naspers also recognises that many countries regulate the collection and use of personal data relating to employees. This Human Resources Data Privacy Policy ("this Policy") describes a baseline set of common principles governing the handling of Human Resources personal data within the Naspers Group.

1.2. Where country-specific additions to this Policy are warranted to assure local compliance, they will be permitted and should be communicated by the relevant Group company to its employees, as required by law. This approach is aligned with the Naspers Board-approved Legal Compliance Policy in the context of Human Resources personal data protection.

2. WHAT THIS POLICY COVERS

2.1. This Policy applies to all personal data about past, present, temporary and permanent employees, contractors, consultants and trainees ("you") that is collected, maintained or used by directors, officers, managers and employees of any Naspers Group company ("we/us") as part of an actual or past employment relationship.

2.2. Personal data collected and used in the context of recruitment activities of prospective employees and candidates is processed in accordance with the Naspers Talent Acquisition Privacy Statement.

2.3. Personal data collected, maintained or used outside of the employment relationship, such as personal data arising from your use of our investees' consumer products or commercial offerings, is not covered by this Policy.

2.4. Nothing in this Policy is intended to form a contract of employment or otherwise. At our discretion and as necessary, we may amend this Policy from time to time. We will notify you when updates are made.

3. OUR APPROACH

3.1. We value our employees and appreciate the importance of treating personal data as confidential.

3.2. In this Policy we outline our global standards for Human Resources personal data privacy practices so that you have an opportunity to understand our approach. We require any directors, officers, managers and employees entrusted with your personal data as part of their job responsibility to treat it as confidential and in conformity with this Policy.

3.3. It is your responsibility to treat any personal data you process in the context of your work with us in a confidential and secure manner, in accordance with all applicable Naspers Group policies, including this Policy.

3.4. We will also seek to ensure that any third-party service providers we use to administer our Human Resources programmes, as described in Section 6 below, are bound to maintain confidentiality when handling your personal data on our behalf, in a manner that is consistent with this Policy.

4. PERSONAL DATA CATEGORIES

4.1. We generally process the following personal data about you over the course of recruitment or employment.

4.1.1. Your biographical information, including your name, gender, date of birth, details of family members, previous job history, education details, nationality

4.1.2. Your contact information, including your home and postal address, telephone number, email address, country of residence

4.1.3. Your identification numbers, including government-issued identification number or passport information

4.1.4. Your performance information, including management metrics, appraisals, feedback

4.1.5. Communications, connections and usage of Information Technology (IT) resources, like your correspondence and details of internet connections, and uses held on- or made through- Naspers systems, including through interactions with tools and platforms powered by Artificial Intelligence (AI),,subject to relevant restrictions under applicable law

4.1.6. Payroll information, including your salary details and bank account information.

4.1.7. Other personal data, e.g. in the context of internal communication tools, surveys, engagement programmes and similar in circumstances where you volunteer to identify yourself. In the context of surveys and engagement programmes, it is generally our practice to allow participation on an anonymous basis

4.2. We most often collect personal data about you directly from you in the course of your application and employment. We may also use other sources, subject to restrictions under applicable law, to assist in obtaining relevant personal data about you.

4.3. For example, third parties help to support recruitment, credit checks, reference and background checks, investigations of possible employee wrongdoing, and help us to locate former employees and beneficiaries for purposes of administering certain benefits plans.

4.4. We may also collect your personal data as a result of monitoring of the use of IT resources for security purposes, adherence to fair use policies and prevention of cyber threats.

4.5. Additionally, we may collect your personal data as a result of monitoring for legal compliance purposes, including in the context of investigating claims related to violations of applicable laws.

4.6. Our Human Resources programmes require personal data about you to function properly. In limited circumstances some programmes may involve certain sensitive health information (e.g. medical certificates submitted to us or other health-related benefits processes), financial data (e.g. payroll) or data about race or religion when mandated by local laws. Such sensitive personal data will be treated with the utmost care and in accordance with special requirements set out in applicable data protection and other laws, including the European Union's General Data Protection Regulation ("GDPR").

4.7. We will endeavour to collect only the minimum amount of personal data required to administer our programmes and to comply with applicable employment and other relevant laws.

5. LAWFULNESS

Generally, Naspers Group companies process your personal data because it is necessary to do so to implement an employment agreement between you and the company, and where our legal duties as an employer require it. In other circumstances, we may process your personal data where it is necessary for us to defend, prosecute or make a claim in a court of law. We may also process personal data for something called "legitimate interests" under European law. In practice, this means that we must put in place appropriate privacy safeguards to ensure that we are respecting your interests, as well as your fundamental rights. Where we take this latter approach, it is our policy to document the assessment we have made and the privacy measures that are in place so that you can review these upon request by contacting our Data Protection Office (See Section 10). Finally, we may seek your explicit consent for an activity from time to time, which you may decline if we ask, or revoke even after you have previously agreed, by contacting your Human Resources representative.

6. HOW WE USE THIS DATA

6.1. Your personal data may be used for the following employment-related purposes:

6.1.1. To contact you and manage our relationship with you, oversee compliance with policies and applicable law, assess performance, for promotions and appraisals and for training purposes

6.1.2. To store emails and documents generated by you on systems that we administer and make available to you, including tools and platforms powered by Artificial Intelligence (AI), for employment related purposes, which may contain personal data

6.1.3. To manage your benefits, including administering remuneration, relocation, insurance, payroll, pensions and other employee benefits and tax, including disclosure to other Group companies and to others such as payroll providers, accountants, occupational health providers, insurers, pensions administrators, hosting service providers and legal advisers

6.1.4. To manage recruitment of employees, including legal eligibility for work, vetting, hires, promotion and succession planning

6.1.5. To comply with policies, including in relation to claims, disciplinary actions or legal requirements;

6.1.6. To conduct investigations and incident response, including reviewing your communications and individually assigned business IT resources in accordance with relevant internal policies related to such investigations and applicable law

6.1.7. For security purposes, in particular prevention and detection of external and internal threats and vulnerabilities, for providing IT support and for employee authentication

6.1.8. To manage occupational health and absence and fitness for work and notifying family members in emergencies

6.1.9. To comply with our legal obligations and to change our business structure we may disclose your personal data in connection with proceedings or investigations anywhere in the world to third parties, such as public authorities, law enforcement agencies, regulators and third-party litigants. We may also provide relevant parts of your personal data to any potential acquirer of or investor in any part of Naspers' business for the purpose of that acquisition or investment

6.1.10. To facilitate business travel, travel-related support including conference attendance, bookings, and emergency support services

6.1.11. To conduct certain checks, such as anti-fraud checks where this is relevant to your position and in accordance with applicable law. We and other organisations engaged by us may access and use your personal data to conduct these credit checks and checks to prevent fraud and money laundering

6.1.12. To process your submissions made through our Speak Up policy should you choose to identify yourself, and to assess and investigate such submissions – in accordance with this Policy and the Speak Up privacy terms

6.1.13. To monitor equal employment opportunities, in respect of diversity categories including but not limited to age, gender, ethnicity, nationality, religion, disability, sexual orientation, and marital or family status. Such monitoring would only apply where it is either required or authorized by the specific country's legislation, and conducted in full compliance with data protection requirements governing the use of such categories of personal data

6.1.14. To manage collective agreements for administering collective employee arrangements where these are in place

6.1.15. For internal and external auditing, assurance and risk management purposes

6.1.16. For statistical analysis and research purposes in the context of employment, including predictive modelling and people planning.

7. INFORMATION SHARING & TRANSFER

7.1. Your personal data will be shared within our Group for the purposes described in Section 5 above to the extent necessary to carry out these purposes, and as permitted by law.

7.2. We are a global Group with a global footprint. Note that your personal data may be processed either locally in the jurisdiction where you work or reside, or in any other jurisdiction where we or our approved third-party service providers operate, worldwide, depending on the needs of the business

over the course of your tenure with us, to the extent necessary and as permitted by law. Should your personal data move outside the European Economic Area or another jurisdiction that restricts the international transfer of personal data, we use GDPR- and locally-compliant mechanisms to require that the same level of data protection be applied in the jurisdiction where the data is being processed.

7.3. Your personal data will only be shared outside our Group with third parties under the following circumstances: (1) where a third-party service provider retained by us is under contract to assist in administering our Human Resources and/or IT activities, subject to appropriate confidentiality obligations and data processing agreements, compatible with this Policy; (2) in the event that the company, business or division in which you are employed is being considered for outsourcing or sale, and then only subject to contractual requirements to preserve confidentiality; (3) with private or government authorities only when we have determined that we are required to do so under applicable laws; (4) to investigate suspected fraud or illegality, to anticipate or defend legal claims; or to conclude a change of control of your company, business or division; or (5) where you have given us your prior permission to do so.

8. WHAT ARE YOUR DATA SUBJECT RIGHTS?

8.1. **SUBJECT ACCESS**: You have the right to access your personal data in many circumstances, generally within 1 month of your request

8.2. **RECTIFICATION**: You can ask us to have inaccurate personal data amended

8.3. **ERASURE**: You can ask us to erase personal data in certain circumstances, recognising that Naspers must in any case respect its data retention legal obligations in the field of employment

8.4. **WITHDRAWAL OF CONSENT**: You can withdraw any consents to processing that you have given us and prevent further processing if there is no other legitimate ground upon which Naspers can process your personal data

8.5. **RESTRICTION**: You can require certain personal data to be marked as restricted for processing in certain circumstances

8.6. **PORTABILITY**: You can ask us to provide you with a copy of your personal data in a such a form that you can send it to a third party

8.7. **RAISE A COMPLAINT**: You can raise a complaint about our processing with the data protection regulator in your jurisdiction, or with our Data Protection Office (see Section 10 below).

9. DATA SECURITY

9.1. Maintaining the security and integrity of your personal data is a high priority and we endeavour to maintain appropriate administrative, technical, personnel and physical measures to safeguard personal data against loss, theft, and unauthorized uses or modifications.

9.2. We expect you to contribute to the security culture of our Group by following appropriate security policies and procedures, completing assigned trainings, and reporting suspected incidents to relevant incident response contacts promptly.

10. DATA RETENTION

We keep records of your personal data no longer than necessary for the purpose for which we obtained them and for any other permitted compatible purposes, including compliance with legal obligations in the field of employment law. Group records management schedules document the applicable retention periods. We use these schedules to establish the retention time periods for various categories of records that contain your personal data. These can be consulted by contacting our Data Protection Office (see Section 10 below).

11. CONTACTS

11.1. At Group-level, the controller of your personal data is Prosus Services B.V. located at Gustav Mahlerplein 5, 1082 MS Amsterdam. The Naspers Group's supervisory authority is the Netherlands data protection authority (Autoriteit Persoonsgegevens (Autoriteit Persoonsgegevens – https://autoriteitpersoonsgegevens.nl).

11.2. Additionally, if you are employed by one of the subsidiaries or affiliates of the Naspers Group, that company will also be a controller of your personal data -processed pursuant to such relationship- and shall provide you with appropriate notice and contact information directly should you wish to contact them or to contact your local data protection authority.

11.3. To exercise your data subject rights, or if you have questions about this Policy, please send an email to our Data Protection Office at: hrprivacy@Naspers.com

11.4. If there are any updates or changes in your personal data please notify us by contacting your Human Resources representative so that we can maintain its accuracy.