Data Privacy Governance Policy

Protecting data subjects

NASPERS

28 November 2023

NASPERS

Data Privacy Governance Policy

Protecting data subjects

1. OBJECTIVES

This policy sets out the approach to data privacy within the Naspers Group 1. It applies to all Naspers Group majority owned or controlled subsidiaries.

The objectives of this policy are:

- to define and document how data privacy is managed in the Group, to support our sustainability priorities, and to demonstrate our governance approach in the context of our public listings;
- to promote best practice with respect to the processing of personal data within the Group;
- to accommodate diversity with respect to business models, resources, culture and legal requirements, and
- to support trust in our businesses' products and services.

The term "data privacy" is used in this policy as an umbrella term to encompass concepts of autonomy, privacy, data protection, security and responsible data management.

The term "personal data" is used in this policy to describe any information relating to an identified or identifiable natural person ("data subject"), consistent with Article 4(1) of the European Union's General Data Protection Regulation ("GDPR").

2. GROUP STATEMENT

Naspers recognises privacy as an important value, and as an essential element of public trust.

We strive to be a trusted company and expect all our businesses to seek that same status. We expect each business to implement responsible data privacy practice in a way that is adapted to its own circumstances which takes account of its business model, the culture of the countries in which it operates, its compliance obligations, and its human and financial resources.

3. ACCOUNTABILITY

Individual businesses directly manage data privacy within their organisations.

CEOs in the Group hold ultimate responsibility for the success of their businesses and therefore must demonstrate leadership over how data privacy is looked after in their organisations.

Each business is responsible for implementing this policy and should designate an individual or set of leaders with responsibility for data privacy within the relevant business.

The Group provides oversight and guidance while also setting policy to ensure that activities happen within a framework that is benchmarked to global standards. Group-level support and monitoring activities are described in Section 6 of this policy

[1] The policy is aligned with the Naspers Legal Compliance Policy, Risk Management Policy, Security Policy, the Naspers IT Governance Charter and the Naspers Sustainable Development Policy

4. DATA PRIVACY PRINCIPLES

The Group expects all businesses to respect and implement each of the following data privacy principles:

Principle 1: Notice

We should offer appropriate notice about our data privacy practices.

Often, the notice takes the form of a privacy policy or privacy statement. Such statements allow data subjects to understand what information is collected, for what purposes, and to hear about how the rest of the principles are applied.

Principle 2: Individual Control

We should honour data subjects' choices about their personal data.

We should support data subjects' desire to control personal data about themselves, and should be responsive to their requests within bounds of technical feasibility and reasonability.

Principle 3: Respect for Context

We should recognise that data subjects' expectations about fair and ethical use of their personal data are informed by the context in which their data was first collected.

Where legally required (and where practicable if there is no legal requirement), we seek permission before using personal data for new purposes that are incompatible with the original context in which they were collected, to avoid unwelcome surprise.

Principle 4: Limited Sharing

We should limit unnecessary personal data sharing with third parties.

We should only allow sharing under controlled circumstances. Specifically, we should only share with third parties if the personal data will be protected subject to the same standards that we use ourselves, and where the sharing is consistent with the data subjects' reasonable expectations.

Principle 5: Retention

We should retain personal data only for as long as we need it.

It is important to have a defined time period in place that is tied to the purposes for which the personal data have been collected, and which is proportionate.

Principle 6: Security

We should ensure appropriate security.

Although no systems can ever be rendered invulnerable to attack, we should ensure that known threats are accounted for, and that we implement administrative, technical, personnel and physical measures to safeguard personal data against loss, theft and unauthorised uses or modifications.

Principle 7: Governments

We should engage with governments responsibly.

It is important to ensure that we have procedures in place to handle government requests to access personal data in a consistent and lawful manner

Principle 5: Retention

We should retain personal data only for as long as we need it.

It is important to have a defined time period in place that is tied to the purposes for which the personal data have been collected, and which is proportionate.

Principle 6: Security

We should ensure appropriate security.

Although no systems can ever be rendered invulnerable to attack, we should ensure that known threats are accounted for, and that we implement administrative, technical, personnel and physical measures to safeguard personal data against loss, theft and unauthorised uses or modifications.

Principle 7: Governments

We should engage with governments responsibly.

It is important to ensure that we have procedures in place to handle government requests to access personal data in a consistent and lawful manner.

Many countries maintain strict data protection laws. All businesses implementing these principles are expected to do so in accordance with applicable laws, in a manner consistent with our Group Legal Compliance Policy.

Our Human Resources functions, through the full lifecycle of employee management, should be accountable to our employees to uphold these same principles when they process employee personal data.

5. DATA PRIVACY PROGRAMMES

A data privacy programme builds on the above principles to help put them into practice. Each business is expected to implement a data privacy programme that is proportionate to the size, scale, geography and resources of its operation. At a minimum, each programme should reflect the following elements:

Element 1: Executive Buy-in

The senior management should emphasise the importance of data privacy and its relationship to trust, brand, growth, risk and compliance to their teams. The CEO should designate a data protection lead or team of individuals responsible for data protection, define where they are best placed within the organisation, and ensure sufficient resources are devoted to privacy programme management.

Element 2: Know your Data

The business should know what personal data it holds and for what purposes it processes that data. The systems used to manage the personal data should also be known, and access rights to the personal data should be clearly defined.

Element 3: Policy-Setting
Certain policy documents should be adopted to support the implementation of the privacy principles. These should include, at a minimum: a consumer privacy policy, a Human Resources privacy policy, a security policy and a data breach/incident response plan.

Element 4: Training Employees
Offering privacy training that informs employees about the above company policies, the principles – and how their roles are impacted by data privacy requirements – should be part of employee onboarding and/or annual training.

Element 5: Vendor & Third-party Management
Where personal data sharing is to be permitted, teams should be prepared to: **(a)** scrutinise their prospective partners to evaluate compatibility with the principles and their own policies, **(b)** require confidentiality and/or data processing agreements to ensure an adequate level of protection for data that are shared, and **(c)** audit vendors based on risk-based criteria.

Element 6: Legal Compliance
Legal advisors should support the business by helping to ensure that applicable laws and their specific requirements are met.

Element 7: Reporting
Each business should be able to demonstrate its compliance with the principles, the Data Privacy Programme elements, and with applicable data protection laws, and should be prepared to report on the above to Group executives, internal audit, the Naspers Board Committees and Board, or to external Regulatory authorities, as appropriate.

6. GROUP SUPPORT AND MONITORING

The Group's Data Privacy Office helps to support businesses with their privacy programme implementations, legal compliance efforts, regulatory engagements, specialised privacy impact assessments and any data privacy implications of mergers and acquisitions activity.

Once data privacy programmes are established, each business should coordinate with the Group internal audit function to verify and document that the above processes continue to function as designed.

The Group requires biannual privacy and security status reports to Group executives as an integral component of ongoing business reviews.

The Risk Committee of the Naspers Board of Directors reviews this policy and its implementation on an annual basis, as part of its oversight and governance responsibilities.

For more information about this policy, please contact the Naspers Group Data Privacy Office at **privacy@naspers.com**