FAQs: GDPR, Data Privacy & Cybersecurity Governance

prosus

Q: What is the Prosus approach to setting policy in the Group?
A: We require individual businesses to directly manage data privacy and security within their organisations. CEOs in our 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. Additionally, our Prosus Board of Directors establishes approved privacy and security frameworks that majority owned/controlled entities must follow. These are set forth in our Data Privacy Governance Policy and in our Cybersecurity Policy.

Q: Why does Prosus believe setting a Group-level policy on privacy is important?
A: We recognise 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 practices in a way that is adapted to its own circumstances, which takes account of its business model, the cultures of the countries in which it operates, its compliance obligations, and its human and financial resources. Having a policy to help guide newer digital companies on how they can benchmark to global best practices is also useful in this effort.

Q: Is Prosus subject to the GDPR?
A: Yes. We are established in the Netherlands, and our corporate operations are indeed subject to the requirements of the European Union's General Data Protection Regulation.

Q: Are Prosus subsidiaries subject to the GDPR?
A: Prosus has investments around the world, and therefore different data protection laws apply to different investments in our portfolio. It is the policy of our Group that all subsidiaries must fully comply with the data protection laws of the jurisdictions in which they operate. To the extent that any Prosus subsidiaries satisfy the requirements of Article 3 of the GDPR, specific to territorial scope, they are subject to the requirements of the GDPR. Subsidiaries that do not independently satisfy the requirements of Article 3 are not.

Q: Does Prosus use the GDPR as an informal group standard?
A: While many global data protection laws draw on the GDPR for inspiration, we do not impose the GDPR as a group standard where it does not otherwise apply as a matter of law. Rather, we emphasize the importance to our subsidiaries of compliance with local laws in the jurisdictions where they operate. In addition, we have established specific global standards in our **Data Privacy Governance** and **Cybersecurity** policies that can be found on our website.

Q: For companies that are subject to the GDPR, does your policy require companies to comply with all of its principles, for example the concepts of purpose limitation, data minimisation and accuracy?
A: Yes. Our group policy incorporates elements informed by several global sources, including the GDPR. To the extent that any specific legal regime's principles or requirements are not explicitly (or implicitly) mentioned in our policy, we have made

it clear in the policy itself that all businesses must implement their programmes in accordance with applicable laws (see Sections 4 and 5). This means that where a law requires a specific principle to be incorporated in order to fully meet its requirements (as in the case of the GDPR), our businesses must do so.

Q: Are the privacy programmes of Prosus businesses limited to only those elements described in the Data Privacy Governance Policy?
A: The policy describes a baseline set of expectations that we believe small and large organizations alike can and should satisfy, even if they may be operating in a jurisdiction without applicable data protection law. The global approach also prepares businesses for the rigor of expectations set by customers and regulators in foreign (non-domestic) markets. For more mature organizations, multinationals, and those operating in regulated environments, the Legal Compliance component of Section 5 of our Policy expands the range of activities that a company will likely be required to undertake. These often include, for example, managing international data transfers, data localization requirements, responding to exercise of subject rights requests of access, correction or deletion of personal data held by the organization, and mandatory data breach notifications.

Q: What is the Prosus approach to Security?
A: At Group level, there are multiple sources that inform security frameworks. Section 4 (Principle 6) and Section 5 (Element 3) of the Data Privacy Governance Policy explicitly acknowledges security as a privacy principle and an essential element of privacy programmes. Further, the objective of the dedicated Cybersecurity Policy is to support the cyber resilience of our businesses. This policy framework incorporates best practices structured around governance, protection, vigilance and resilience.

Q: In the event of an incident, do you report significant data breaches?
A: Many jurisdictions in which we operate (including those subject to GDPR) impose specific reporting requirements on us in the event of a data breach. As stated in our Cybersecurity Policy, each entity in the Group is expected to define and implement an incident response plan that denotes the roles and responsibilities (and contact information) of key leaders tasks with managing data incidents broadly, and security incidents specifically. These leaders take responsibility for liaising with our legal team and with authorities on notifications, as appropriate, in compliance with legal obligations.

Q: Who can I contact if I have questions about Prosus data privacy or cybersecurity policies, or with compliance questions?
A: Please reach out to us at privacy@prosus.com

Q: Who can I contact if I want to report a suspected security problem in one of the Prosus companies?
A: Please reach out to us at cyber@prosus.com