Acer Group Personal Data Protection Management Policy

This Policy is promulgated to regulate the collection, processing, utilization and cross-border transmission of personal data by Acer Group, to avoid infringement of privacy regulations and to enhance reasonable use of personal data.

1. Organization: Head Quarter and each Regional Office of Acer Group shall establish a data protection team and/or a cybersecurity team with data protection function and shall set out roles and responsibilities for the management of personal data.
2. Management System: Acer Group shall establish and implement procedures and a security management system for collecting, processing and utilizing personal data. Acer Group's collection and processing of personal data shall comply with the principles of transparency, necessity, purpose limitation and accuracy. Unless otherwise approved by Acer Global Data Protection Team, Acer Group entities shall not collect customers' personal information related to credit cards or similar payment tools and shall not engaged in selling of personal data.
3. Protecting Data Subject's Rights: Head Quarter and each Regional Office of Acer Group shall accept and handle requests from data subjects who exercise their rights under applicable data protection laws and regulations. Acer Group shall also provide channels for complaint submission and procedures for handling damage compensation.
4. Security Mechanism: Acer Group shall establish and implement security management procedures for storage, deletion, disposal and transmission of personal data. Access control and activity logs for personal data shall be duly implemented and maintained by Acer Group.
5. Incident Response Procedure: Head Quarter and each Regional Office of Acer Group shall establish and implement incident response procedures for prevention, forensic investigations, notification and response for personal data breach incidents. The procedure shall comply with the requirements of applicable laws and regulations related to personal data breach incidents.
6. Risk Management Mechanism:

   Acer Group shall:

   (1) implement personal data risk management and carry out personal data inventory check and risk assessment.

   (2) provide education and training for personnel in charge of personal data processing activities and deploy security control for personal data processing equipment.

   (3) carry out Information security exercise and drill from time to time.

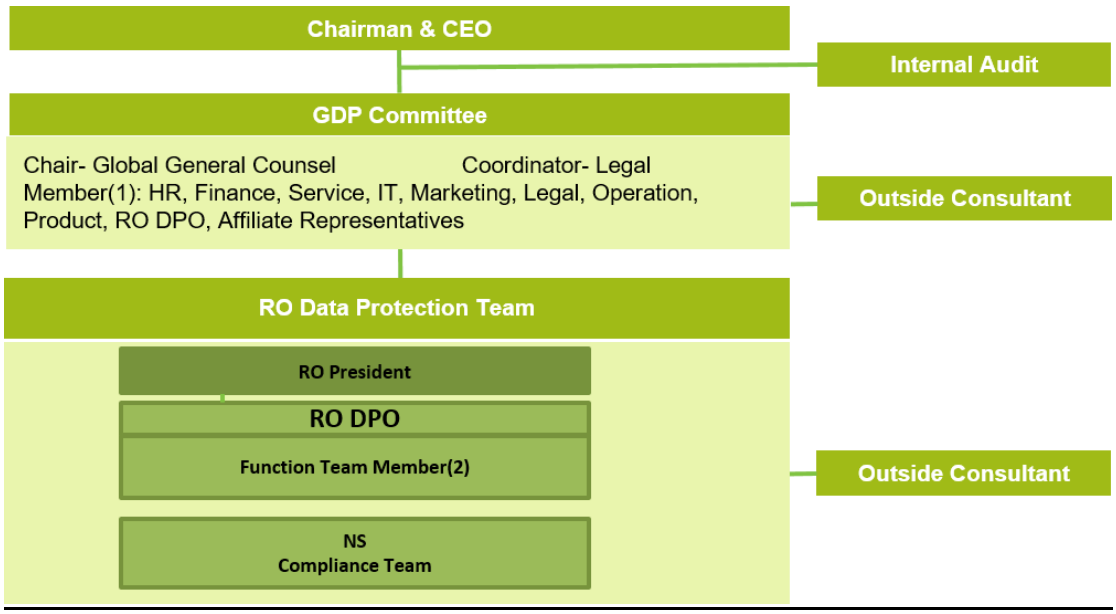
(4) require and supervise outsourced parties' compliance with personal data protection regulations.

7. Internal and External Audit: Acer Group shall conduct periodical internal audit on personal data management and consistently improve the personal data management system. If necessary, Acer Group may engage external professionals to carry out personal data management assessment and audit.
8. This policy takes effect after the approval by the CEO of Acer Group. Amendments may be made in order to adapt to the changes of applicable personal data protection laws and regulations around the globe or to meet actual implementation needs.

Annex: Organization Chart and Roles & Responsibilities

Annex: Organization Chart and Roles & Responsibilities

1. Global Data Protection ("GDP") - Organization Chart



(1) GDP members include the Heads of Global HR, Finance, Service, IT, Marketing, Operation, Product BG Head, RO DPO, and Affiliate Representative(optional).

(2) RO Function team members will be identified by RO DPO, however, Legal, HR, Finance, Service, IT, Marketing, Operation, Logistic and Product team representative shall be included.

2. Global Data Protection ("GDP") - Roles & Responsibilities

Organization/Roles	Responsibilities
GDP Committee	(1) Propose global policies for Chairman & CEO's final approve. (2) Internal Announcement (3) Training and Drill (Planning) (4) Management of any global or cross-RO incident (5) Audit Plan and Co-work with internal and external auditors (6) Ensuring privacy by design to enforce data protection from day 1 of a new project/product
Chair of GDP Committee	(1) draft global data protection policies and SOP for Committee's review and discussion (2) Monitor global data protection compliances (3) Design, Build and maintain a e-system for global data protection compliance (4) Lead the global/cross-RO incident
RO DPO & Team Members	(1) NS laws and regulations collection for GDP Committee reference (2) RO GDP compliance (3) RO audit, training and drill execution (4) Guide and support NS compliance
The Executives	(1) Review and approve global or RO policies, guidelines or rules (2) Final decision on incident management
Function Team Members	(1) Support GDP Committee, Chair of GDP Committee and RO DPO (2) Liaise with the NS point of contact
NS Compliance	(1) Collection and update any laws and regulations (2) Support training, drill and audit (3) Other local compliance matters