宏碁集團個人資料保護管理政策

Acer Group Personal Data Protection Management Policy

為規範 Acer Group 個人資料之蒐集、處理、利用及國際傳輸，避免違反隱私保護法規並促進個人資料之合理利用，特訂定本政策。

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. 組織：宏碁集團總部與各區域營運總部應設立個人資料保護管理組織或設立兼管資料保護之網路資訊安全組織，並應制定個人資料管理相關權責與職掌。

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. 管理制度：宏碁集團應建立與執行個人資料蒐集、處理及利用之程序與安全維護管理制度。蒐集與處理個人資料應符合透明、必要、合目的性及正確性等原則。非經宏碁集團全球個人資料管理組織之特別許可，宏碁集團不蒐集顧客信用卡或類似支付工具等個人資料，且不得涉及出售個人資料。

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. 保障個資所有人之權利：宏碁集團總部與各區域總部應依相關個資準據法規定受理當事人可行使之權利請求，並提供申訴管道與損害賠償處理程序。

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. 安全機制：宏碁集團應建立與執行個人資料儲存管理、刪除、處置與傳輸等安全管理程序，落實個人資料存取控管權限及軌跡留存。

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. 應變程序：宏碁集團應建立與執行個人資料事故之預防、鑑識、通報及應變管理程序，確保符合相關法規對事故應變處理之要求。

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. 風險管理機制:

宏碁集團應：

(1) 落實個人資料風險管理，執行個人資料盤點及風險評估。
(2) 落實個人資料處理經辦人教育訓練及處理個人資料的設備安全控管。
(3) 不定期實施資安測試演練。
(4) 確實監督受託委外廠商遵循個人資料保護管理規定

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. 內外部稽核機制：定期執行個人資料管理內部稽核，持續改善個人資料管理制度，以及視需求委託外部專業機構執行個人資料管理評估及稽核。

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.

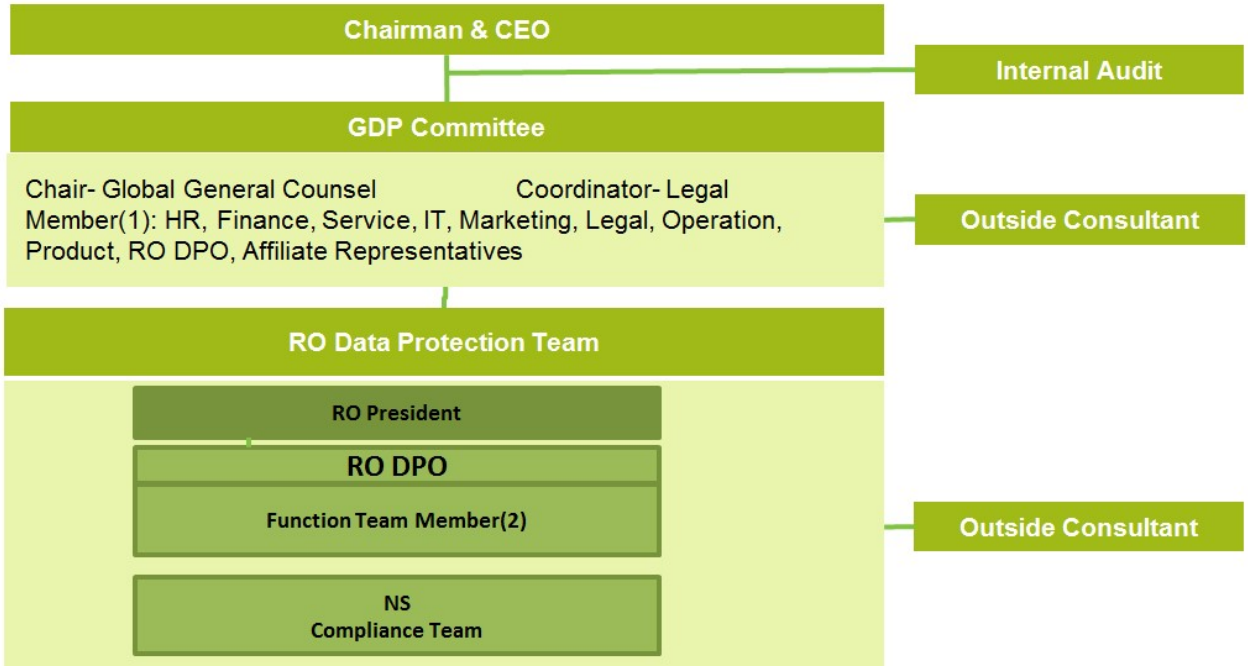
8. 本管理政策經宏碁集團執行長核准後頒訂施行，並得視全球個資保護相關法令之變更或實際執行需求而修訂之。

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