系統資料隱私強化說明文件

系統資料隱私強化設計是一項以保障用戶資料和機密信息為目標的系統設計策略，涵蓋技術、流程及合規性等多方面。以下從資料生命周期管理、技術控制措施及組織合規策略等角度詳細說明如何設計與實施：

1. 資料生命周期管理

針對資料的存取、傳輸、使用及銷毀實施嚴格的控制。

1.1 資料分類與標記

- **分類標準**：基於資料敏感性進行分級，如公共資料、內部資料、機密資料及高度機密資料。
- **標記方法**：透過標籤、元數據或內嵌式標記技術自動標示資料類型。

1.2 最小權限原則

- **限制存取**：採用角色為基礎的存取控制（RBAC）或屬性為基礎的存取控制（ABAC），確保僅授予完成特定工作的必要權限。
- **動態調整**：依使用者需求動態調整權限，並記錄變更操作。

2. 技術控制措施

2.1 資料加密

- **傳輸加密**：採用 TLS 1.3 或更高版本，確保資料傳輸過程的完整性和保密性。

2.2 資料遮蔽（Data Masking）

- 在非生產環境中，利用遮蔽技術生成隱匿數據，防止開發測試人員接觸真實數據。
- **動態遮蔽**：依存取者身份在實時呈現前遮蔽敏感信息。

2.3 偵測與防範

- **入侵偵測系統（IDS）/入侵防禦系統（IPS）**：識別和阻止可疑的資料存取行為。

- **資料洩漏防護（DLP）**：防範未授權的資料外洩，特別是經由電子郵件、文件共享等管道。

2.4 匿名化與去識別化

- 匿名化：不可逆處理，例如刪除個人標識符。
- 去識別化：使用不可逆函數隱匿身份特徵，但能在必要時重新識別。

3. 組織與流程強化

3.1 日誌與稽核

- **詳細記錄存取日誌**：監控敏感資料的存取，包括時間、地點、存取者和操作詳情。
- **定期稽核**：採用內部及外部稽核以檢視資料保護是否符合標準（如 ISO 27001）。

3.2 使用者教育與意識提升

- 定期培訓員工了解隱私規定及合規要求，提升潛在安全風險識別能力。
- 提供針對性測試，例如模擬釣魚郵件，檢測反應能力。

3.3 法規合規

- 遵循相關資料保護法規，如 GDPR（一般資料保護法）、CCPA（加州消費者隱私法）、HIPAA（健康隱私法）等。

Azure Cloud 強化隱私保護機制

Azure 提供多層次機制來強化隱私保護，確保用戶的數據安全：

1. 數據加密

靜態和傳輸中的數據均默認加密。支援透明數據加密（TDE）和 Azure 磁碟加密，並支援 Bring Your Own Key（BYOK）。

A. **靜態數據加密：**存儲在磁碟或資料庫中的數據透過自動加密保護，如透明數據加密（TDE）和 Azure Storage Service Encryption，使用 AES-256 加密標準。
B. 傳輸中數據加密：透過 TLS/SSL 協議確保數據在客戶端與 Azure 服務之間的通信安全。
C. 自帶密鑰選項（BYOK）：客戶可透過 Azure Key Vault 管理並使用自己的加密密鑰。
D. 雙層加密：部分服務支持多層加密，確保額外的保護。

2. 隱私管理工具

Azure Policy 和 Azure Purview 提供數據分類和合規性工具，用於管理隱私需求。

A. Azure Purview：提供數據分類、標籤和發現功能，讓用戶了解數據位置、結構和敏感性。
B. Azure Policy：確保服務和數據符合隱私標準（如 GDPR），強制執行合規性規則。
C. Azure Key Vault：集中管理和保護加密密鑰、憑據與證書。
D. Azure Monitor：追蹤系統訪問與活動，快速檢測違規行為。

3. 網路隔離

透過 Azure Private Link、虛擬網路（VNet）和服務端點限制 Internet 連線。

A. 虛擬網路（VNet）隔離：每個資源都可以部署在隔離的虛擬網路中，

確保內部通信與公用網絡分離。

B. Private Link：透過專用私有端點連接 Azure 服務，避免數據流量經由公共網絡。
C. 服務端點：允許虛擬網路中的資源安全地連接到 Azure 服務。
D. 網絡安全群組 (NSG)：細粒度控制進出 VNet 的流量。
E. 防火牆及應用網關：提供進一步的威脅保護和數據隱私。

4. 訪問控制

使用基於角色的訪問控制（RBAC）和 Microsoft Entra ID 確保權限最小化。

A. 基於角色的存取控制（RBAC）：授權用戶最低必要權限，確保按職責劃分訪問權限。
B. Microsoft Entra ID：提供單一登入 (SSO)、多重身份驗證 (MFA) 等身份管理。
C. 條件式存取：基於用戶、位置、設備等條件限制登錄和資源使用。
D. 資源鎖定與審核日誌：防篡改敏感設置，並記錄所有訪問行為進行監控。

5. 合規性

Azure 符合國際隱私法如 GDPR，並定期接受第三方審核。

A. 全球標準支持：Azure 符合多項隱私和安全合規標準（如 GDPR、HIPAA、ISO 27001 等），並經常接受獨立第三方審查。
B. 透明性與控制：透過工具（如 Azure Compliance Manager），用戶可追踪其資源的合規狀態並執行改善措施。
C. 數據主權保障：提供多區域數據存儲選擇，用戶可以確保數據存放在符合地域要求的地方。
D. 定期更新：Azure 平台持續監控法規變化，確保其服務與最新要求一致。

Google Cloud 強化隱私保護機制

GCP 在強化隱私方面採用多層次機制，確保用戶的數據安全：

1. 數據加密

靜態數據和傳輸中數據均默認加密，採用 AES-256 加密標準；支持客戶自帶密鑰（BYOK）和客戶管理加密密鑰（CMEK）功能。

A. 靜態加密：所有數據在存儲時都會加密，使用 AES-256 等強加密標準。
B. 傳輸中加密：所有數據在進行網絡傳輸時均會透過 SSL/TLS 協議加密。
C. 密鑰管理：用戶可以通過 Google Cloud Key Management 服務管理和輪換加密密鑰，也支持客戶自帶加密密鑰（BYOK）。
D. 透明加密：實現加密無縫集成，無需用戶干預。

2. 隱私管理工具

提供 Data Loss Prevention API 用於發現和屏蔽敏感數據。

A. Data Loss Prevention（DLP）API：自動識別、分類並保護敏感資料。
B. Cloud Identity & Access Management（IAM）：控制誰能夠存取資源和資料。
C. Cloud Security Command Center：提供集中化的安全與隱私監控功能。
D. Audit Logs：詳細記錄數據存取和操作，以進行審計和監控。

3. 存取控制

提供 Data Loss Prevention API 用於發現和屏蔽敏感數據。

A. 身份與存取管理（IAM）：細粒度的權限控制，確保只授權必要的用戶存取數據。
B. 條件式存取：基於特定情況（如地理位置或設備狀態）控制存取。

C. 最小權限原則：限制用戶、應用或服務的權限，以減少暴露風險。

D. 單一登入（SSO）和多因素驗證（MFA）：強化身份認證與存取安全。

4. 數據主權

在 Google Cloud 的數據主權原則中，用戶控制數據位置是核心。用戶可選擇將數據存儲於符合地域性法規的區域，這有助於滿足如 GDPR 等法律要求。此外，Google Cloud 還提供全球多區域選擇，使客戶能確保數據存儲符合數據主權和法律合規性要求。這確保了數據存儲位置的透明性與主權管理。

5. 合規保障

符合全球標準，如 GDPR 和 ISO。

A. 全球標準符合性：Google Cloud 具備符合 GDPR、ISO 27001、HIPAA 等國際隱私和安全法規的合規認證，保證服務提供符合多種法律要求。

B. 透明審核和報告：提供完整的合規報告與安全性審核，以協助企業確保其服務符合相關規範。

C. 合規性工具：如 Google Cloud Compliance Center，讓用戶監控其資源的合規狀態，確保適應法規變更。

Amazon Web Services 強化隱私保護機制

AWS 在強化隱私方面採用多層次機制，確保用戶的數據安全：

1. 數據加密

提供靜態和傳輸中數據的加密服務（如 AES-256），並支持用戶自帶密鑰（BYOK）。

A. 靜態數據加密：AWS 提供加密存儲選項，如 Amazon S3 和 EBS，加密用戶的靜態數據，並使用標準 AES-256 加密演算法。
B. 傳輸中加密：使用 TLS/SSL 協議來加密數據在網路中的傳輸，保護數據免受中途截取。
C. 密鑰管理：AWS Key Management Service（KMS）和自帶密鑰（BYOK）選項幫助用戶管理和控制加密密鑰。

2. 隱私管理工具

透過 AWS Identity and Access Management（IAM）控制權限，確保只有授權用戶能訪問數據。

A. 身份與訪問管理（IAM）：允許設置精細的權限策略，根據用戶角色控制其對 AWS 資源的存取。
B. 最小權限原則：確保用戶只具有完成任務所需的最低權限，減少隱私風險。
C. 多因素認證（MFA）：加強身份驗證，防止未經授權的存取。
D. 條件性存取：設置基於位置、時間等條件的訪問規則，提高安全性。

3. 合規性管理

AWS 符合全球多項標準，並透過 AWS CloudTrail 提供詳細的合規審計日誌。

A. 合規標準遵循：AWS 遵循多種國際標準，如 GDPR、HIPAA、ISO 27001 等，確保產品與服務符合法律法規要求。
B. 自動化合規工具：AWS 提供如 AWS Artifact 和 AWS Config 這些工

具，協助用戶維持合規性，並生成合規報告。

C. 審計與日志管理：利用 AWS CloudTrail 追蹤和審核 API 操作，提升監控能力。