FOXIT ESIGN 合規性概述

某些組織需要遵守一系列特定 的監管要求，而 Foxit eSign 可作為用於履行合規性義務的關鍵組成部分。本文件按區域和產業概述 Foxit eSign 支援遵守的各種法規。

白皮書

目錄

按區域

美國

Foxit eSign 完全符合美國所有 ESIGN 法案和 UETA 合規性法規，並提供重要工具來協助確保您的文件具有法律約束力。

- 清晰的簽名關聯記錄和簽名歸屬 (稽核追蹤)
- 定義的文件保留原則
- 為每個簽署文件提供完結證書
- 為使用者提供輕鬆的方式來證明以電子方式簽署和執行業務的明確意圖

請務必記住，雖然 Foxit eSign 軟體可協助您遵守 ESIGN 和 UETA 法律，但它可能不足以滿足您當地、州政府、國際市場或產業要求。請務必隨時查看相關的指導方針。

加州消費者隱私法案 (CCPA)

Foxit eSign 遵守加利福尼亞州規定的《加州消費者隱私法案》(CCPA)，其中涉及消費者知情權、存取權、刪除權、選擇退出權、個人資訊不受任何經營業務的公司歧視的權利，以及為加州消費者傳輸資料的權利。

Foxit eSign 已證明其在此類資料方面嚴格遵守 CCPA。我們將通知客戶其用戶端的任何請求，並將根據法律規定在客戶同意的情況下採取必要措施。

歐盟

根據歐洲單一市場交易的歐盟法規規定，我們將嚴格遵守「電子身分識別、驗證和信任服務」(eIDAS)。

eIDAS 第 910/2014 號法規定義了三個主要的電子簽名層級：基本合規性、進階電子簽名 (AES) 和合格的進階電子簽名 (QES 或 QAES)。

*基本合規性：*屬於此層級的簽名通常包括核取方塊或輸入您的姓名，不需要任何進一步的技術通訊協定。

*進階電子簽名 (AES)：*對於進階電子簽名，簽署者的簽名直接與文件相關聯，所有變更都受到監控和記錄，並使用數位認證流程來驗證簽名。

*合格的進階電子簽名(QES 或 QAES)：*這是最高層級且最符合條件的電子簽名。此層級保證了私密簽署金鑰，可確保用於建立簽名的資料只能使用一次，防止偽造，並允許簽署者保留對簽名流程的完全控制。合格的簽名無法更改、複製或重現，且維持受到合格信任供應商的監督。

Foxit eSign符合進階電子簽名 (AES) 和合格電子簽名 (QES) 規定的必要條件。*

*Foxit eSign 透過 ZealiD 提供 QES。ZealiD 堅持遵守基於 eIDAS 認證的信任服務、eIDAS 指定的 ETSI 標準和尖端的歐盟遠端識別規定的資料安全性策略。

GDPR

身為 Foxit eSign 客戶，您擁有以下由 GDPR 法律規定且受 Foxit eSign 保護的權利：

- 有權確認是否處理您的個人資料。
- 有權更正不準確的資料和完成不完整的個人資料。
- 在某些情況下，有權立即刪除您的個人資料。
- 在某些情況下，有權限制處理您的個人資料。

- 根據您的特定情況反對我們處理您個人資料的權利，但僅限於處理的法律依據是該類處理具有必要性：出於公共利益執行工作或行使賦予我們的任何官方權力；我們或第三方追求合法利益的目的。
- 有權反對處理您的個人資料以進行直接行銷目的。
- 有權根據您的特定情況，反對我們出於科學或歷史研究目的或統計目的處理您的個人資料，除非出於公共利益的原因執行工作所必需進行的處理。

Foxit eSign 提供以下功能來協助客戶遵守 GDPR：

存取[1] – 使用者或簽署者的大部分個人資訊可以由個人透過 Foxit eSign 的使用者介面直接存取，也可以由在簽署文件時請求資訊之組織的授權方存取。

更正 – 收集的使用者或簽署者的所有個人資訊均可透過使用者介面獲得。如果需要進行變更，使用者和簽署者可以在簽署文件時直接進行變更。簽署者可以在簽署任何文件後發起變更，方法是請求授權寄件者對其記錄進行審閱/更新或重新發起另一個簽名請求。

刪除 – 根據使用者在簽署事件中的角色不同，採取的措施會有所不同。傳送合約的使用者必須向其僱用公司提出刪除請求。Foxit eSign 不會控制雇主在交易期間收集的資料。簽署流程在簽署事件期間收集有關簽署者的以下資訊：姓名、電子郵件地址和 IP 位址。此資訊與他們簽署的合約儲存在一起，並由傳送合約的公司控制。如果簽署者需要與透過該合約收集的個人資訊有關的資訊，則需要聯絡合約的寄件者。Foxit eSign 無法為簽署者提供有關合約或向其傳送該合約的公司的任何資訊。如果簽署者認為傳送方有不配合之情事，Foxit eSign 可以代表簽署者聯絡寄件者並協助刪除，但寄件者必須分享寄件者嘗試失敗的證據。

---

[1] Foxit eSign 使用符合 SOC 2 Type 2 和 PCI 標準的 SSAE16 設施，維護深受信賴的美國和歐洲資料中心。在美國，資料中心位於北維吉尼亞州 (美國東部)、俄亥俄州 (美國東部) 和北加利福尼亞州 (美國西部)。在歐洲，資料中心位於德國法蘭克福。

按產業

HIPAA (醫療保健)

Foxit eSign 已通過 HIPAA 認證，可協助確保您和您患者的私密和敏感文件始終處於監管範圍內。為維護個人識別資訊 (PII)，Foxit eSign 提供安全欄位來遮罩此資訊。我們利用加密和 Token 化來防止 PII 資料洩漏。所有資料以靜態和動態方式進行加密。每個 Foxit eSign 簽名交易都包含一個完全可追蹤的防篡改稽核追蹤，並獲得了完結證書。

儲存於 SOC 2 稽核資料中心內的文件使用 AES 256 標準在客戶文件的應用程式層級進行加密，以確保完全機密性。

Foxit eSign 根據 Pro 和 Enterprise 方案提供業務聯盟合約 (BAA)。

此外，Foxit eSign 還遵守 HIPAA 法規，體現在以下方面：

- 具有法律約束力的電子簽名 (根據 UETA 和 ESIGN) 將在法庭上具有法律效力
- 嚴格遵守 HIPAA 電子安全性標準
- 詳細的文件標準，包括來源和身分驗證、加密金鑰、鎖定文件的雜湊演算法以及其他支援合規性的簽名技術
- 透過全面稽核，追蹤每個文件的動態和簽名

21 CFR 第 11 條 (生命科學)

對於符合 FDA 21 CFR 第 11 條合規性的使用者，Foxit eSign 將支援遵守本法規，遵循 FDA 制定的電子簽名使用法規並提供滿足要求所需的功能和工具。簽署者的身分驗證是在簽名時驗證每個首字母，方法是在存取文件以供簽署的同時，在執行初始身分檢查後至少提供登入密碼。一旦收件人簽署了文件，就會以電子方式儲存，並附上包含簽名影像、重要事件時間戳記和簽署者 IP 位址的完結證書。

Foxit eSign 遵守 21 CFR 第 11 條的規定，體現在以下方面：

- 身分驗證方法
- 詳細的稽核追蹤
- 文件防篡改、防偽
- 時間戳記
- 為簽署的文件提供完結證書

FERPA (教育)

透過 Foxit eSign，教育工作者和管理員能夠輕鬆地符合 FERPA 要求，確保資料的安全性和可存取性，以適應為滿足記錄請求而提出的 45 天要求。此外，Foxit eSign 還支援 FERPA，體現在以下方面：

- 為學生提供一種電子方式來簽署 FERPA 所需的發佈表單，透過防篡改和防偽功能維護記錄的安全性和完整性
- 為學校提供一種安全且簡單的方式來收集學生和家長簽署的學生記錄發佈同意書
- 提供符合 ESIGN 和 UETA 且具有法律約束力的解決方案
- 提供詳細的稽核功能、簽名完結證書和數位簽署金鑰，以便學校可以預防欺詐性簽名並有效確保有效性，同時滿足驗證電子簽名的 FERPA 要求
- Foxit eSign 提供安全欄位以遮罩個人識別資訊 (PII)，並使用加密和 Token 化來防止 PII 資料洩露
- 所有資料都採用靜態和動態加密方式

FERPA (金融)

Foxit eSign 支援遵循 FINRA 規定 4512，包括 FINRA 2019 監管通知增修條款 19-13 和規定 17a-4(f) 的文件保留要求，這意味著您可以確保文件傳送和簽署始終符合產業法規。Foxit eSign 支援 FINRA 合規性，體現在以下方面：

- 提供獲得所有主要銀行認可、符合 ESIGN 和 UETA 且具有法律約束力的解決方案
- 發佈具有 256 位元加密的防篡改和防偽數位簽名，確保如果有人試圖更改文件，都有記錄證明
- 實行嚴格的 SOC 2 Type 2 稽核和合規性並嚴格遵守 AICPA 制定的 5 項信任服務原則
- 提供全面而詳細的稽核，顯示寄件者和簽署者採取的所有操作，包括日期、時間和地點
- 為所有文件提供詳細的完結證書
- 提供身分驗證方法選項，例如雙因素驗證 (2FA) 和基於知識的驗證 (KBA)
- 允許使用者儲存和下載已完成的簽署文件以保留記錄

PCI DSS

支付卡產業資料安全標準 (PCI DSS) 是一種資訊安全標準，適用於處理來自主要信用卡計劃的品牌信用卡的組織，以加強對持卡人資料管理的控制並減少欺詐行為。Foxit eSign 始終遵守 PCI DSS 3.2.1，滿足並超過了保護信用卡持有者資料處理的要求。此外，Foxit eSign 會定期進行最高層級的安全風險測試，包括「十大安全漏洞清單 (OWASP Top 10)」中的安全風險。