大江生醫股份有限公司

隱私權政策

大江生醫完成 ISO/IEC 27001:2022 驗證， 且 ISMS 覆蓋企業營運關鍵之公司網路、ERP 系統與機房作業。透過相關機制，將管理系統落實為可持續運作的資安治理並進一步擴大至子公司，推動集團資安管理一體化。

身為以研發與製造為本的生技企業，我們深知個人資訊的機密性與信任基礎，並理解資料於跨國營運、數位服務與供應鏈協作中的重要性。因此，我們承諾以合法、正當與透明的方式處理個人資訊，並依據歐盟《一般資料保護規範》（GDPR）以及臺灣《個人資料保護法》及其施行細則等相關規範，建立一致且可持續改善的隱私保護機制。

本政策所稱「您」或「資料主體」，係指與本公司具有業務往來或僱傭關係之自然人，包括本公司員工、客戶、供應商等利害關係人。

本政策適用範圍涵蓋本公司及各海外子公司與營運據點之營運活動中，涉及個人資訊處理之相關作業。同時，我們在針對弱勢市場群體（例如兒童、市場知識匱乏者等）的營銷傳播方面，將盡力避免造成誤導，避免使其對產品或服務可能帶來的益處產生誤解。

我們的承諾

我們承諾以「最小必要」與「目的限定」為核心原則處理個人資訊，並將個人資訊保護與資訊安全風險納入整體風險管理與合規管理架構，透過制度化治理、內外部檢視與持續改善，確保保護措施與營運需求同步精進。

- 合法、正當、透明：於適用法令允許與目的必要範圍內蒐集與使用個人資訊，並清楚告知處理目的與方式。
- 最小必要與目的限定：僅蒐集與處理完成特定目的所必要的個人資訊，避免不必要或過度處理。

- 安全與韌性：採取合理且適當的技術與組織措施，維護個人資訊之機密性、完整性與可用性。
- 權利尊重：保障資料主體依 GDPR 等法令所享有之權利，並依規定時程與程序回應。
- 跨國傳輸與第三方管理、公開透明與持續改善：因跨國營運需要而進行資料傳輸或委外處理時，要求相關對象採取相應保護措施並遵循本政策；並以內部稽核與管理審查等機制定期檢視執行情形，必要時提出並落實改善方案。

在資訊安全方面，本公司已取得 ISO/IEC 27001 資訊安全管理系統認證，並由獨立第三方認證機構定期查核與驗證。

我們的策略

治理與責任

建立隱私保護與資訊安全之治理架構，明確角色與責任分工，並納入合規與風險管理流程，以確保政策落實、資源配置與管理成效可被監督與追蹤。

資料最小化與全生命週期管理

依「最小必要」原則進行資料蒐集、使用與保存；在目的達成或保存期間屆滿後，依規定採取刪除或其他適當處置，以降低資料暴露風險；同時，我們將盡力採取合理之技術與管理措施，確保僅於本政策所列目的必要之期間內進行處理，並僅於最短必要期限內加以保存。

資訊安全與風險管理

以資訊安全管理系統為基礎，定期進行風險評估、內部稽核與管理審查，針對識別之風險提出改善措施並持續追蹤成效。本公司建立個人資料安全事件之應變與通報機制，並依適用法令之規定履行相關通報與告知義務。

跨國傳輸與第三方管理

於合乎本政策所列目的範圍內，基於跨國營運需要，可能將個人資料傳送至本公司集團內其他公司及其設立據點所在之國家 / 地區；同時，於必要時與外部顧問、服務供應商等合作，並依目的與法律程序與主管機關等共享資料；該等國家 / 地區之法律規定與個資保護

要求可能不同；我們將採取相當之保護措施，確保跨國傳輸與委外處理過程維持一致之保護水準。

資料主體權利與申請處理

本公司提供資料主體權利行使之正式途徑，並依適用法令規定之期限與程序回應；資料主體依法享有之其他權利，本公司亦將依適用法令予以保障。

利害關係人溝通、教育與正向效益

透過溝通與教育提升內外部利害關係人對隱私保護的認知，強化資料倫理與信任，並以公開透明方式揭露政策與管理作法的持續精進方向。

透明告知

我們將依據 GDPR 與適用法令，就個人資訊處理向您清楚說明以下事項，並在必要時提供適當的補充資訊：

資料控制者與處理者

資料控制者為大江生醫股份有限公司；於業務需要時，可能委託服務供應商等第三方作為資料處理者，並要求其遵循本政策與適用法令。

個人資訊之收集目的

包括履行契約關係或契約前措施、依法令或主管機關要求履行義務、以及基於本公司或第三人之正當利益且不侵害您的權利與自由之前提下之必要處理。

個人資訊之類別

可能包括基本識別資料、聯絡方式、交易與合約資料、線上服務使用資訊等，並以最小必要原則處理。

使用期間、範圍、對象及方式

於合法前提下，為營業目的、網站營運或提供產品 / 服務，可能於集團內共享資料，並在必要時分享予主管機關、外部顧問、服務供應商、訴訟或法律程序相關方、為調查或預防犯罪所必要之第三方，或提供廣告、外掛程式或網站內容之第三方；另因跨國性業務需

要，個人資料可能傳送至本公司集團營運所在之各國家 / 地區；前述跨國傳輸之國家 / 地區可能有不同之法律規定與個資保護要求；我們將採取相當之保護措施，確保資料在傳輸過程中維持一致的保護水準。 此外，我們將盡力採取合理措施，僅於達成前述目的所必要之期間內處理並在最短必要期限內保存；目的達成或保存期間屆滿後，將依規定刪除、匿名化或採取其他適當處置。

資料主體權利

包括查詢與閱覽（及製給複本）、補充與更正、限制處理 / 停止處理或反對處理、刪除等；惟於符合法令所定例外情形下，本公司得於必要範圍內繼續留存或處理。

是否提供個人資訊之自由與可能影響

您得自由選擇是否提供個人資訊；惟如拒絕提供或資訊不足，可能影響身分確認、資格審查、契約履行、法定申報或其他營運所必須之作業，進而影響服務提供或權益。