資料處理協議

https://scratcher.io/zh-tw/data-processing-agreement

標準版本，最後更新於 2026 年 10 月 22 日。當您使用 Scratcher 時，本資料處理協議為您與 Scratcher ApS（CVR 38552864，Fruebjergvej 3, 2100 Copenhagen Ø, Denmark）之間協議的一部分，其內容依 GDPR 第 28 條之要求擬定。

資料處理協議

本資料處理協議為客戶與 Scratcher 之間協議的組成部分。若本資料處理協議附於該協議，則條款與細則第 10 條不適用，改適用本資料處理協議。

1. 定義

1.1. 除非上下文明確另有要求，本資料處理協議中下列首字母大寫之用語，應具有以下含義：

- 「資料外洩」指任何意外或非法違反個人資料安全之事件，導致所處理之個人資料遭意外或非法銷毀、遺失、更改，或未經授權（未獲許可）之揭露或存取。
- 「資料控制者」指依 GDPR 之定義，決定個人資料處理之目的與方式的客戶。
- 「資料處理者」指代表資料控制者處理個人資料的 Scratcher。
- 「個人資料」指與已識別或可識別之自然人有關的任何資訊（GDPR 第 4(1) 條），且為資料處理者依協議代表資料控制者所處理者。
- 「GDPR」指歐洲議會及歐盟理事會於 2016 年 4 月 27 日通過、關於保護自然人個人資料處理及此類資料自由流通，並廢止指令 95/46/EC 之規章（EU）2016/679（一般資料保護規則）。
- 「子處理者」指除資料處理者之員工外，由資料處理者聘用、於資料處理協議所訂範圍及目的內，依其指示代表資料處理者處理個人資料之任何人。

1.2. 上述未定義之首字母大寫用語，除非上下文明確另有要求，其含義與協議中之定義相同。

2. 適用範圍

2.1. 本資料處理協議所載之條款與條件，適用於資料處理者代表資料控制者並依其指示處理個人資料之情形。

2.2. 本資料處理協議提及資料處理者之處，相關規定亦適用於資料處理者所聘用之任何子處理者。

3. 資料控制者之指示與處理條件

3.1.

資料處理者僅得依資料控制者之書面記錄指示處理個人資料，包括將個人資料傳輸至第三國之情形，但資料處理者依法須遵循歐盟或成員國法律另有要求者除外。於此情形下，資料處理者應於處理前將該法律要求告知資料控制者，但該法律基於重大公共利益而禁止提供此類資訊者除外。

3.2.

資料處理者應處理資料控制者（包括其客戶）於使用服務時上傳或提交之各類當事人的個人資料。代表資料控制者所處理之個人資料類型及當事人類別，列於本資料處理協議之附錄 A。

3.3.

雙方同意，將本資料處理協議以及資料控制者於使用服務時可能成立之協議，視為資料控制者之書面記錄指示。資料控制者得透過調整服務設定，就個人資料之蒐集向資料處理者提供其他書面記錄指示。雙方亦得以書面約定執行資料控制者之額外指示及其價格。

3.4.

資料處理者應自資料控制者於使用服務時上傳或傳送個人資料之時起，處理該個人資料，直至其被移除為止，但不得超過本資料處理協議第 12 條所訂之期間。

3.5. 若資料處理者認為某項指示違反 GDPR 或歐盟或成員國之其他資料保護規定，應立即通知資料控制者。

3.6. 資料控制者承諾，經資料處理者要求，應立即提供資料處理者為代表資料控制者處理個人資料時，妥善遵守 GDPR 所有要求所需之任何資訊、文件或協助。

4. 個人資料之保密

4.1.

資料處理者僅得為提供服務及行使其於協議下之權利之目的使用個人資料。除法律另有要求外，資料處理者不得向第三方揭露個人資料。

4.2.

資料處理者應確保，僅有因履行職務或為資料處理者提供服務而需要該等資料之資料處理者員工或供應商，方可存取個人資料，且所有獲授權處理個人資料之人員均已承諾保密，或負有適當之法定保密義務。

4.3.

若資料處理者為遵守法律要求而有義務向第三方（例如執法機關）揭露個人資料，除法律另有要求外，資料處理者應立即將揭露個人資料之要求告知資料控制者。

4.4. 上述保密義務於本資料處理協議終止後仍然有效。

5. 技術與組織措施

5.1.

考量最新技術水準、實施成本，以及處理之性質、範圍、情境與目的，並考量對自然人權利與自由造成之不同可能性與嚴重程度的風險，資料處理者應於處理個人資料之前及處理期間的任何時間，實施確保個人資料安全所需之適當技術與組織措施。於選擇及實施技術與組織措施以確保適當安全等級時，資料處理者尤應考量因處理當事人之個人資料、因所傳輸、儲存或以其他方式處理之資料遭意外或非法銷毀、遺失、更改、未經授權之揭露或非法存取所產生之風險。

5.2. 由於資料處理者為其領域之專業人士，並具備提供服務之知識與經驗，資料處理者應選擇並決定達成本資料處理協議第 5.1
條所訂目標所需之技術與組織措施，但該等措施無論如何均應符合適用法律之要求。儘管如此，資料控制者有權就技術與組織安全措施之應用向資料處理者提出指示與建議。資料處理者應考量並審酌資料控制者之該等建議，並 (i)
就資料處理者將如何落實資料控制者之指示，向資料控制者提供附有理由之回覆，且 (ii) 立即採取措施實施該等措施。

5.3. 資料處理者於簽訂本資料處理協議時所實施之技術與組織措施，載於附錄 C。資料處理者維持通過 ISO/IEC 27001 認證之資訊安全管理系統，且得隨時間更新各項措施，惟整體安全等級不得因此降低。

5.4. 考量處理之性質及其所掌握之資訊，資料處理者應協助資料控制者確保遵守 GDPR 第 32 條所定之義務。

6. 資料處理稽核

6.1. 資料處理者應向資料控制者提供證明其遵守 GDPR 第 28 條所定義務所需之一切資訊，包括其現行有效之 ISO/IEC 27001 證書，並於經要求時提供其適用性聲明書（Statement of Applicability）。

6.2. 為查核資料處理者是否妥善處理個人資料，資料控制者有權於下列條件下對該處理作業進行查核：(i)
稽核僅限於個人資料之處理；(ii) 資料控制者須於合理期間內通知資料處理者其欲進行稽核之意願，該期間不得少於 4 週；(iii) 稽核之進行方式不得干擾資料處理者之日常運作；(iv) 稽核費用由資料控制者負擔；(v)
稽核須由獨立人士執行，其人選須事先經資料處理者核准（核准不得無理拒絕），且該人士須承諾保護資料處理者之機密資訊。

6.3.

資料處理者有權就其協助進行稽核獲得報酬。報酬金額由資料處理者考量其因稽核所產生之成本後決定。資料處理者應於稽核前將報酬金額告知資料控制者。

6.4. 由有權之監督機關進行之稽核與查核，不受第 6.2 條及第 6.3 條所訂條件之限制。

6.5.

若資料控制者對稽核結果不滿意，資料控制者有權依非訴訟程序單方終止本資料處理協議及協議。於此情形下，終止該等協議將是資料控制者得採取之唯一措施，資料處理者無義務賠償資料控制者之任何損害。

7. 子處理者

7.1.

資料控制者茲授予資料處理者一般性事先同意，得聘用子處理者，由其於本資料處理協議所訂範圍及目的內，代表資料處理者處理個人資料。

7.2.

資料處理者應確保已與所聘用之子處理者簽訂書面協議，約定子處理者承諾遵守與本資料處理協議所載相同之資料保護義務，尤其應提供充分保證，以使其實施適當之技術與組織措施，令處理作業符合 GDPR
之要求。資料處理者應就子處理者履行義務之情形，對資料控制者負責。

7.3. 子處理者之現行名單載於本資料處理協議之附錄 B。資料處理者應於預定更換或聘用新子處理者之事件發生前至少 14 個曆日，向資料控制者提供相關資訊，以通知其該計畫。

7.4. 若資料控制者於收到資料處理者依本資料處理協議第 7.3
條所訂程序發出之通知後，在子處理者更換或新聘用後仍繼續使用服務，則視為資料控制者已同意資料處理者之該等行為。若資料控制者不同意該子處理者之更換或參與，資料控制者有權以非訴訟程序單方終止協議。於此情形下，終止協議將是資料控制者得採取之唯一措施，資料處理者無義務賠償資料控制者之任何損害。

7.5.

若資料控制者撤回其聘用子處理者之一般性同意，資料處理者有權以非訴訟程序單方終止協議，且該終止應視為基於重大事由所為，並視為資料控制者並未因該終止而受有任何損害。

8. 資料外洩

8.1.

資料處理者應就影響個人資料之任何資料外洩，以銷售提案中所載之電子郵件地址通知資料控制者；若未載明，則以資料控制者帳號擁有者之電子郵件地址通知，並應於得知資料外洩後不得無故延遲，且最遲於 24
小時內為之。考量所提供服務及個人資料處理之性質與可得之資訊，資料處理者應向資料控制者提供下列資訊：(i)
資料外洩之性質，包括在可能的情況下，受影響當事人之類別及其大概人數；(ii) 資料外洩可能造成之後果；(iii)
資料處理者已實施或建議採取以因應資料外洩之措施，包括在適當情況下，減輕資料外洩可能造成之不利後果的措施；(iv)
資料保護長或可提供進一步資訊之任何其他聯絡人之全名及聯絡資料。

8.2. 資料處理者應記錄所有資料外洩，包括與資料外洩有關之事實、其影響及所採取之矯正措施。於 GDPR
或其他適用法規所定之情形下，資料處理者應向監督機關提供該等記錄。

8.3. 考量處理之性質及其所掌握之資訊，資料處理者應協助資料控制者確保遵守其於 GDPR 第 33 條及第 34
條下之義務。資料控制者仍負責通知監督機關，並於必要時通知當事人。除資料外洩係因資料處理者違反其於本資料處理協議下之義務所致外，資料處理者於第 8.1 條所訂通知以外之協助，可能須另行收費。

9. 將個人資料傳輸至第三國

9.1.

資料處理者將個人資料傳輸至第三國（歐盟／歐洲經濟區以外）時，僅得依資料控制者之書面記錄指示為之，且無論何時均應遵守 GDPR 第五章之規定。

9.2. 資料控制者核准附錄 B

所列之子處理者，即構成對該等子處理者依該處所述進行之傳輸之書面記錄指示。每次該等傳輸均應以歐盟執委會之充足性認定（包括適用於經認證接收方之歐盟與美國資料隱私框架）、歐盟執委會之標準契約條款，或 GDPR
第五章下之其他傳輸機制為依據。

10. 合作

10.1. 考量所提供服務之性質、客戶資料之處理及可得之資訊，資料處理者應與資料控制者合作，以確保履行 GDPR 第 32 至 36 條所訂之義務。為此，且僅於本資料處理協議所訂範圍內，資料處理者應向資料控制者提供其妥善履行 GDPR
下義務所需之所要求資訊。

10.2.

若處理之類型（尤其是使用新技術），並考量處理之性質、範圍、情境與目的，可能對自然人之權利與自由造成高度風險，資料處理者應於處理前，協助資料控制者就所擬處理作業對個人資料保護之影響進行評估。

10.3.

若當事人、監督機關或第三方依法要求資料處理者提供有關所處理個人資料之任何資訊，資料處理者應不得無故延遲地將該等要求轉交資料控制者。資料處理者承諾於必要範圍內協助資料控制者回應當事人、監督機關或第三方之要求，並履行資料控制者與落實當事人權利有關之義務，包括但不限於個人資料之更正權及刪除權、個人資料之可攜權、反對及限制處理之權利。資料處理者應確保其所持有之資訊於法定期限內傳達。

11. 資料控制者之義務

11.1.

資料控制者應自行裁量並自負責任，決定提供給資料處理者之個人資料類型及當事人類別，且僅應向資料處理者提供其妥善提供服務所必要之個人資料。資料控制者應承擔一切相關風險，包括資料處理者收到超過必要範圍之個人資料之風險。

11.2.

資料控制者聲明並保證，其已取得並將於協議期間內持續維持向資料處理者提供個人資料，以及依協議委託資料處理者處理個人資料所需之一切許可與授權。

12. 個人資料之刪除與返還

12.1.

於協議或本資料處理協議終止時，資料處理者應依資料控制者之選擇，刪除代表資料控制者所處理之所有個人資料，或將所有個人資料返還資料控制者（資料控制者可隨時從服務中匯出其資料），並刪除任何現有副本，且向資料控制者證明其已完成上

述作業，但歐盟或成員國法律要求保留個人資料者除外。備份中的副本將於備份依正常週期到期時刪除，且在此之前不會用於任何其他目的。

13. 責任

13.1.

無論資料控制者遭受何種損害，資料處理者於本資料處理協議下之全部責任應限制如下：資料處理者及其任何供應商就因本資料處理協議而生或與之相關之任何及所有請求所負之總責任，不得超過資料控制者於引發請求之事件發生日前十二（12）個月內，實際就服務支付予資料處理者之金額。在適用法律允許的最大範圍內，資料處理者或其供應商於任何情況下均不對任何特殊、附帶、間接或衍生性損害（包括但不限於利潤、資料或其他資訊之損失、營業中斷、人身傷害、隱私權喪失所致之損害）負責，即使資料處理者或供應商已被告知可能發生該等損害，且即使救濟措施未能達成其基本目的亦然。

13.2. 第 13.1 條之限制僅適用於雙方之間。其不適用於依適用法律無法限制之責任，亦不影響當事人依 GDPR 第 82 條所享有之權利。

14. 效力與終止

14.1.

本資料處理協議自協議生效時起生效，並於協議持續有效期間內持續有效。資料處理者之義務，於其代表資料控制者處理個人資料期間持續有效。

15. 最終條款

15.1. 資料處理者應於預定變更本資料處理協議前至少 30 天通知該變更。若資料控制者於變更公告後繼續使用服務，則視為資料控制者同意對本資料處理協議之變更。若資料控制者不同意該等變更，資料控制者將無法使用服務，並有權終止協議。

15.2. 若本資料處理協議與協議之間有所衝突，就個人資料之處理而言，以本資料處理協議為準。

15.3. 本資料處理協議之準據法及爭議解決方式，與協議中所訂者相同。

15.4. 附錄：

- 附錄 A：個人資料處理之詳細說明；
- 附錄 B：經核准之子處理者；
- 附錄 C：技術與組織措施

附錄 A – 個人資料處理之詳細說明

標的與期間	於協議期間內，與服務有關之個人資料處理，以及其後直至個人資料依第 12 條被刪除或返還為止。
處理之性質	代管與儲存；透過資料控制者之活動與表單蒐集個人資料；於服務中顯示、匯出及刪除；依資料控制者之設定向參加者發送電子郵件與訊息（例如確認信、代碼及獎品通知）；依資料控制者之指示，透過整合、Webhook 及 API 傳輸至資料控制者自有系統；支援與錯誤處理。
個人資料處理之目的	讓資料控制者能依協議約定使用資料處理者之服務
個人資料處理作業	蒐集並儲存客戶資料，包括使用服務時所提供之個人資料
個人資料之類型	名字、姓氏、電子郵件、IP 位址及由其推得之大概位置、註冊日期與時間（建立時間），以及生日和電話號碼等其他資料（如由客戶蒐集）。依資料控制者設定其活動之方式，另包括活動問題的答案、遊戲結果與所贏得之獎品、代碼、同意紀錄、參加者上傳之檔案（例如圖片），以及瀏覽器與裝置資訊等技術資料。
特種類別資料	非預期處理。除非另以書面約定，資料控制者不得透過服務蒐集特種類別個人資料（GDPR 第 9 條）或有關刑事定罪之資料（GDPR 第 10 條）。
當事人類別	資料控制者（客戶）活動之參加者、未註冊之資料控制者活動訪客（IP 位址、大概位置及瀏覽器資訊），以及於代表資料控制者處理其資料之範圍內，資料控制者之服務使用者。
個人資料處理地點	個人資料應於資料處理者之營業場所及位於歐盟境內之虛擬伺服器上處理，並由附錄 B 所列之子處理者於該處所載地點處理。
處理期間／儲存期限	由資料控制者於服務中設定。依條款與細則第 9.4 條，資料處理者得刪除超過三（3）年之個人資料。

附錄 B – 經核准之子處理者

於簽訂資料處理協議時，資料控制者核准聘用下列子處理者。傳輸至歐盟／歐洲經濟區以外之情形，於接收方已通過認證時以歐盟與美國資料隱私框架為依據，否則以歐盟執委會之標準契約條款為依據（第 9.2 條）。

子處理者	處理說明	處理地點
Amazon Web Services EMEA SARL, Luxembourg (AWS)	服務代管：伺服器、資料庫、檔案儲存、備份、快取及記錄檔	歐盟（瑞典斯德哥爾摩）。內容透過 Amazon CloudFront 網路傳遞，該網路可能於歐盟／歐洲經濟區以外之邊緣節點處理流量。
ClickHouse, Inc. (ClickHouse Cloud)	活動統計（如造訪、參加與註冊）之成效分析資料庫，包括 IP 位址及瀏覽器資訊	歐盟（德國法蘭克福），託管於 AWS。
Mailgun Technologies, Inc.（Sinch 旗下公司）	發送資料控制者設定寄給參加者的電子郵件，例如確認信、代碼及獎品通知，並於啟用追蹤時包括寄送、開啟及點擊紀錄	歐盟（郵件資料採歐盟區域）；有限的帳號資訊可能於全球範圍內處理。
ip-api.com	查詢參加者 IP 位址之大概位置，並偵測來自代理伺服器及資料中心之流量，以防止詐欺與機器人	羅馬尼亞（歐盟）；無法排除於歐盟／歐洲經濟區以外處理或傳輸資料。
Google (Gemini API)	服務中的 AI 功能，例如 AI 助理、翻譯及文字生成。除非資料控制者之使用者自行輸入，否則參加者資料僅以假名化或彙總形式傳送（例如姓名縮寫、電子郵件網域及註冊時間）	美國，並可能包括其他國家，視 API 端點及處理設定而定。
Functional Software, Inc. (Sentry)	服務之錯誤監控與工作階段重播，以發現並修正錯誤。報告可能包含內部使用者與帳號 ID，以及資料控制者之使用者瀏覽器之技術資料。工作階段重播中的文字已遮蔽	歐盟（德國，Sentry 歐盟區域）。
Cloudflare, Inc. (Turnstile)	活動表單之機器人防護，僅於資料控制者為活動啟用時使用。接收參加者之 IP 位址及瀏覽器訊號	全球網路；可能於歐盟／歐洲經濟區以外處理。
Features & Labels, Inc. (fal.ai)	服務中的 AI 圖像生成與編輯、去背及配音。接收資料控制者之使用者所提交的提示詞與圖片	美國。
Adressevælger (adressevaelger.dk)	活動表單中的地址建議，僅於資料控制者為活動啟用時使用。接收參加者輸入的地址文字及參加者之 IP 位址	丹麥（歐盟）。

附錄 C – 技術與組織措施

資料處理者維持由 Bureau Veritas 認證、通過 ISO/IEC 27001:2022 的資訊安全管理系統（證書編號 FIHSK27150F）。各項措施包括：

- **代管與實體安全：** 所有客戶資料均儲存於歐盟境內的 Amazon Web Services（AWS）資料中心。資料處理者不自行營運伺服器；實體與環境安全由 AWS 提供，AWS 已通過 ISO 27001 及 SOC 2 認證。
- **網路安全：** 伺服器與資料庫運行於無法從網際網路連線的私有網路（Amazon VPC）中。僅負載平衡器與內容傳遞網路對外公開，並受網頁應用程式防火牆（AWS WAF）及 DDoS 防護保護。
- **加密：** 所有流量均以 TLS（HTTPS）加密。資料庫、檔案及備份以 AES-256 進行靜態加密。整合之憑證另於應用程式層級加密。密碼以 bcrypt 雜湊並加鹽。
- **存取控制：** 針對客戶使用者採角色型存取控制、雙重驗證及 Google 單一登入、工作階段逾時，以及登入嘗試次數限制。員工存取遵循最小權限與必要知悉原則，使用唯一帳號，並於可行時採用多重驗證，至少每年審查一次，且於人員離職時撤銷。
- **隔離：** 客戶資料依帳號進行邏輯隔離（租戶隔離），且每項請求均經授權。
- **記錄與監控：** 基礎架構之變更記錄於防竄改的稽核軌跡中，應用程式記錄集中蒐集，平台全天候受到監控，客戶可於操作記錄中查看其使用者的操作。
- **可用性與韌性：** 每日加密備份至少保留七天，並與正式環境分開儲存，至少每年測試一次還原，並每年審查及演練業務持續運作與災難復原計畫。
- **事件管理：** 具備書面流程以通報、評估、遏止、分析及追蹤資訊安全事件，包括依第 8 條通知資料外洩。
- **安全開發與營運：** 伺服器以不可變容器運行，無 SSH 存取，且絕不以手動方式變更，變更於發布前均經測試。
- **人員：** 員工受保密義務約束，並於資訊安全管理系統架構下接受資訊安全意識訓練。可存取基礎架構之合作夥伴本身亦通過 ISO 27001 認證，且僅取得其工作所需之存取權限。
- **資料最小化與刪除工具：** 資料控制者決定每個活動蒐集哪些資料，並可匯出、刪除或自動刪除參加者資料。