Thỏa thuận xử lý dữ liệu

https://scratcher.io/vi/data-processing-agreement

Phiên bản tiêu chuẩn, cập nhật lần cuối ngày 22 tháng 10, 2026. Thỏa thuận xử lý dữ liệu này là một phần của thỏa thuận giữa bạn và Scratcher ApS (CVR 38552864, Fruebjergvej 3, 2100 Copenhagen Ø, Đan Mạch) khi bạn sử dụng Scratcher. Thỏa thuận được soạn để đáp ứng các yêu cầu của Điều 28 GDPR.

Thỏa thuận xử lý dữ liệu

Thỏa thuận xử lý dữ liệu này là một phần không tách rời của Thỏa thuận giữa Khách hàng và Scratcher. Nếu Thỏa thuận xử lý dữ liệu này được đính kèm vào Thỏa thuận, khoản 10 của Điều khoản và điều kiện sẽ không áp dụng, và Thỏa thuận xử lý dữ liệu này sẽ được áp dụng thay thế.

1. Định nghĩa

1.1. Trừ khi ngữ cảnh yêu cầu rõ ràng khác đi, các thuật ngữ viết hoa sau đây trong Thỏa thuận xử lý dữ liệu này có các nghĩa như sau:

- “Vi phạm dữ liệu” là bất kỳ sự vi phạm nào, do vô ý hoặc trái pháp luật, đối với bảo mật dữ liệu cá nhân, dẫn đến việc hủy, mất, thay đổi hoặc tiết lộ không được phép (không có sự cho phép) đối với Dữ liệu cá nhân đã được xử lý, hoặc dẫn đến việc truy cập trái phép vào Dữ liệu cá nhân đó.
- “Bên kiểm soát dữ liệu” là Khách hàng khi Khách hàng xác định mục đích và phương thức xử lý Dữ liệu cá nhân, theo định nghĩa trong GDPR.
- “Bên xử lý dữ liệu” là Scratcher khi Scratcher tham gia xử lý Dữ liệu cá nhân thay mặt Bên kiểm soát dữ liệu.
- “Dữ liệu cá nhân” là mọi thông tin liên quan đến một cá nhân là người đã được xác định hoặc có thể được xác định (Điều 4(1) GDPR) mà Bên xử lý dữ liệu xử lý thay mặt Bên kiểm soát dữ liệu theo Thỏa thuận.
- “GDPR” là Quy định (EU) 2016/679 của Nghị viện châu Âu và Hội đồng ngày 27 tháng 4, 2016 về bảo vệ cá nhân liên quan đến việc xử lý dữ liệu cá nhân và về việc lưu thông tự do các dữ liệu đó, đồng thời bãi bỏ Chỉ thị 95/46/EC (Quy định chung về bảo vệ dữ liệu).
- “Bên xử lý phụ” là bất kỳ bên nào, trừ nhân viên của Bên xử lý dữ liệu, được Bên xử lý dữ liệu thuê để xử lý Dữ liệu cá nhân thay mặt Bên xử lý dữ liệu và theo chỉ dẫn của Bên xử lý dữ liệu, trong phạm vi và vì các mục đích được nêu trong Thỏa thuận xử lý dữ liệu.

1.2. Các thuật ngữ viết hoa không được định nghĩa ở trên có cùng nghĩa như trong Thỏa thuận, trừ khi ngữ cảnh yêu cầu rõ ràng khác đi.

2. Phạm vi

2.1. Các điều khoản và điều kiện trong Thỏa thuận xử lý dữ liệu này áp dụng cho việc Bên xử lý dữ liệu xử lý Dữ liệu cá nhân thay mặt Bên kiểm soát dữ liệu và theo chỉ dẫn của Bên kiểm soát dữ liệu.

2.2. Khi Thỏa thuận xử lý dữ liệu này nhắc đến Bên xử lý dữ liệu, các quy định liên quan của Thỏa thuận xử lý dữ liệu cũng áp dụng cho mọi Bên xử lý phụ được Bên xử lý dữ liệu thuê.

3. Chỉ dẫn của Bên kiểm soát dữ liệu và điều kiện xử lý

3.1. Bên xử lý dữ liệu chỉ xử lý Dữ liệu cá nhân theo các chỉ dẫn bằng văn bản của Bên kiểm soát dữ liệu, kể cả chỉ dẫn về việc chuyển Dữ liệu cá nhân sang quốc gia thứ ba, trừ khi luật của Liên minh hoặc của Quốc gia thành viên mà Bên xử lý dữ liệu chịu sự điều chỉnh yêu cầu khác. Trong trường hợp đó, Bên xử lý dữ liệu phải thông báo cho Bên kiểm soát dữ liệu về yêu cầu pháp lý đó trước khi xử lý, trừ khi luật đó cấm việc cung cấp thông tin như vậy vì lý do quan trọng về lợi ích công cộng.

3.2. Bên xử lý dữ liệu sẽ xử lý Dữ liệu cá nhân của các nhóm chủ thể dữ liệu mà Bên kiểm soát dữ liệu (bao gồm cả khách hàng của Bên kiểm soát dữ liệu) tải lên hoặc gửi khi sử dụng Dịch vụ. Các loại Dữ liệu cá nhân và nhóm chủ thể dữ liệu được xử lý thay mặt Bên kiểm soát dữ liệu được liệt kê trong Phụ lục A của Thỏa thuận xử lý dữ liệu này.

3.3. Các bên thống nhất xem Thỏa thuận xử lý dữ liệu này và Thỏa thuận được hình thành khi Bên kiểm soát dữ liệu sử dụng Dịch vụ là các chỉ dẫn bằng văn bản của Bên kiểm soát dữ liệu. Bên kiểm soát dữ liệu có thể cung cấp thêm cho Bên xử lý dữ liệu các chỉ dẫn bằng văn bản về việc thu thập dữ liệu cá nhân, bằng cách điều chỉnh cài đặt của Dịch vụ. Các bên cũng có thể thỏa thuận bằng văn bản về việc thực hiện các chỉ dẫn bổ sung của Bên kiểm soát dữ liệu và chi phí của các chỉ dẫn đó.

3.4. Bên xử lý dữ liệu sẽ xử lý Dữ liệu cá nhân kể từ thời điểm Bên kiểm soát dữ liệu tải lên hoặc truyền dữ liệu khi sử dụng Dịch vụ, cho đến khi dữ liệu đó bị xóa, nhưng không vượt quá thời hạn quy định tại Điều 12 của Thỏa thuận xử lý dữ liệu này.

3.5. Bên xử lý dữ liệu phải thông báo ngay cho Bên kiểm soát dữ liệu nếu theo ý kiến của Bên xử lý dữ liệu, một chỉ dẫn vi phạm GDPR hoặc các quy định bảo vệ dữ liệu khác của Liên minh hoặc của Quốc gia thành viên.

3.6. Bên kiểm soát dữ liệu cam kết, theo yêu cầu của Bên xử lý dữ liệu, sẽ cung cấp ngay mọi thông tin, tài liệu hoặc hỗ trợ cần thiết để Bên xử lý dữ liệu tuân thủ đầy đủ các yêu cầu của GDPR khi xử lý Dữ liệu cá nhân thay mặt Bên kiểm soát dữ liệu.

4. Bảo mật Dữ liệu cá nhân

4.1. Bên xử lý dữ liệu chỉ sử dụng Dữ liệu cá nhân nhằm cung cấp Dịch vụ và thực hiện các quyền của mình theo Thỏa thuận. Trừ khi luật yêu cầu khác, Bên xử lý dữ liệu không được tiết lộ Dữ liệu cá nhân cho bên thứ ba.

4.2. Bên xử lý dữ liệu bảo đảm rằng chỉ những nhân viên hoặc nhà cung cấp của Bên xử lý dữ liệu cần đến dữ liệu đó để thực hiện nhiệm vụ hoặc để cung cấp dịch vụ cho Bên xử lý dữ liệu mới được quyền truy cập Dữ liệu cá nhân, và mọi người được ủy quyền xử lý Dữ liệu cá nhân đều đã cam kết giữ bí mật hoặc chịu nghĩa vụ bảo mật phù hợp theo luật.

4.3. Nếu Bên xử lý dữ liệu buộc phải tiết lộ Dữ liệu cá nhân cho bên thứ ba (ví dụ: cơ quan thực thi pháp luật) để tuân thủ yêu cầu của pháp luật, Bên xử lý dữ liệu phải thông báo ngay cho Bên kiểm soát dữ liệu về yêu cầu tiết lộ Dữ liệu cá nhân, trừ khi luật yêu cầu khác.

4.4. Các nghĩa vụ bảo mật này vẫn có hiệu lực sau khi Thỏa thuận xử lý dữ liệu này chấm dứt.

5. Biện pháp kỹ thuật và tổ chức

5.1. Có tính đến trình độ kỹ thuật hiện có, chi phí triển khai, bản chất, phạm vi, bối cảnh và mục đích của việc xử lý, cũng như các rủi ro với xác suất và mức độ khác nhau đối với quyền và tự do của các cá nhân, Bên xử lý dữ liệu sẽ triển khai, trước khi xử lý Dữ liệu cá nhân và vào bất kỳ thời điểm nào trong quá trình xử lý, các biện pháp kỹ thuật và tổ chức phù hợp cần thiết để bảo đảm an toàn cho Dữ liệu cá nhân. Khi lựa chọn và triển khai các biện pháp kỹ thuật và tổ chức nhằm bảo đảm mức an toàn phù hợp, Bên xử lý dữ liệu đặc biệt phải tính đến các rủi ro phát sinh từ việc xử lý Dữ liệu cá nhân của chủ thể dữ liệu, từ việc vô tình hoặc trái pháp luật hủy, làm mất, thay đổi, tiết lộ không được phép hoặc truy cập trái pháp luật vào dữ liệu được truyền, lưu trữ hoặc xử lý theo cách khác.

5.2. Vì Bên xử lý dữ liệu là đơn vị chuyên nghiệp trong lĩnh vực của mình và có kiến thức, kinh nghiệm trong việc cung cấp Dịch vụ, Bên xử lý dữ liệu sẽ lựa chọn và xác định các biện pháp kỹ thuật và tổ chức cần thiết để đạt được các mục tiêu nêu tại khoản 5.1 của Thỏa thuận xử lý dữ liệu này, nhưng trong mọi trường hợp các biện pháp đó phải tuân thủ yêu cầu của luật hiện hành. Tuy vậy, Bên kiểm soát dữ liệu có quyền đưa ra chỉ dẫn và góp ý cho Bên xử lý dữ liệu về việc áp dụng các biện pháp bảo mật kỹ thuật và tổ chức. Bên xử lý dữ liệu sẽ xem xét các góp ý của Bên kiểm soát dữ liệu và (i) đưa ra phản hồi có lý giải cho Bên kiểm soát dữ liệu về cách Bên xử lý dữ liệu sẽ thực hiện các chỉ dẫn đó, (ii) đồng thời thực hiện ngay các bước cần thiết để áp dụng các biện pháp đó.

5.3. Các biện pháp kỹ thuật và tổ chức mà Bên xử lý dữ liệu đã áp dụng tại thời điểm ký kết Thỏa thuận xử lý dữ liệu này được mô tả trong Phụ lục C. Bên xử lý dữ liệu duy trì hệ thống quản lý an toàn thông tin được chứng nhận theo ISO/IEC 27001 và có thể cập nhật các biện pháp theo thời gian, với điều kiện mức độ an toàn tổng thể không bị giảm.

5.4. Có tính đến bản chất của việc xử lý và thông tin mà Bên xử lý dữ liệu có được, Bên xử lý dữ liệu sẽ hỗ trợ Bên kiểm soát dữ liệu bảo đảm tuân thủ các nghĩa vụ theo Điều 32 GDPR.

6. Kiểm toán xử lý dữ liệu

6.1. Bên xử lý dữ liệu sẽ cung cấp cho Bên kiểm soát dữ liệu mọi thông tin cần thiết để chứng minh việc tuân thủ các nghĩa vụ quy định tại Điều 28 GDPR, bao gồm chứng nhận ISO/IEC 27001 hiện hành và, khi có yêu cầu, Tuyên bố về khả năng áp dụng (Statement of Applicability).

6.2. Để xác minh xem Bên xử lý dữ liệu có đang xử lý Dữ liệu cá nhân đúng cách hay không, Bên kiểm soát dữ liệu có quyền tiến hành kiểm tra việc xử lý đó theo các điều kiện sau: (i) cuộc kiểm toán chỉ được liên quan đến việc xử lý Dữ liệu cá nhân; (ii) Bên kiểm soát dữ liệu phải thông báo cho Bên xử lý dữ liệu về mong muốn tiến hành kiểm toán trong một khoảng thời gian hợp lý, và không ngắn hơn 4 tuần; (iii) cuộc kiểm toán phải được tiến hành theo cách không làm gián đoạn các hoạt động hằng ngày của Bên xử lý dữ liệu; (iv) cuộc kiểm toán phải do Bên kiểm soát dữ liệu chi trả; (v) cuộc kiểm toán phải do một cá nhân độc lập thực hiện, và người được đề cử phải được Bên xử lý dữ liệu chấp thuận trước; việc chấp thuận này không được từ chối một cách vô lý; người đó phải cam kết bảo vệ Thông tin bảo mật của Bên xử lý dữ liệu.

6.3. Bên xử lý dữ liệu có quyền nhận thù lao cho việc hỗ trợ thực hiện kiểm toán. Mức thù lao do Bên xử lý dữ liệu quyết định, có tính đến chi phí mà Bên xử lý dữ liệu phải chịu liên quan đến cuộc kiểm toán. Bên xử lý dữ liệu sẽ thông báo cho Bên kiểm soát dữ liệu về mức thù lao trước khi kiểm toán.

6.4. Các cuộc kiểm toán và thanh tra do cơ quan giám sát có thẩm quyền tiến hành không chịu sự ràng buộc của các điều kiện tại khoản 6.2 và 6.3.

6.5. Nếu Bên kiểm soát dữ liệu không hài lòng với kết quả kiểm toán, Bên kiểm soát dữ liệu có quyền đơn phương chấm dứt Thỏa thuận xử lý dữ liệu này và Thỏa thuận theo thủ tục ngoài tòa án. Trong trường hợp này, việc chấm dứt Thỏa thuận là biện pháp duy nhất mà Bên kiểm soát dữ liệu có thể áp dụng, và Bên xử lý dữ liệu không có nghĩa vụ bồi thường bất kỳ thiệt hại nào cho Bên kiểm soát dữ liệu.

7. Bên xử lý phụ

7.1. Bên kiểm soát dữ liệu theo đây cho phép trước và chung cho Bên xử lý dữ liệu thuê các Bên xử lý phụ sẽ xử lý Dữ liệu cá nhân thay mặt Bên xử lý dữ liệu, trong phạm vi và vì các mục đích được nêu trong Thỏa thuận xử lý dữ liệu này.

7.2. Bên xử lý dữ liệu bảo đảm đã ký kết thỏa thuận bằng văn bản với các Bên xử lý phụ đã được thuê, theo đó các Bên xử lý phụ cam kết tuân thủ cùng các nghĩa vụ bảo vệ dữ liệu như những nghĩa vụ nêu trong Thỏa thuận xử lý dữ liệu này, đặc biệt là cung cấp đủ bảo đảm để triển khai các biện pháp kỹ thuật và tổ chức phù hợp, sao cho việc xử lý đáp ứng các yêu cầu của GDPR. Bên xử lý dữ liệu chịu trách nhiệm trước Bên kiểm soát dữ liệu về việc các Bên xử lý phụ thực hiện nghĩa vụ của mình.

7.3. Danh sách hiện tại các Bên xử lý phụ được nêu trong Phụ lục B của Thỏa thuận xử lý dữ liệu này. Bên xử lý dữ liệu sẽ thông báo cho Bên kiểm soát dữ liệu về kế hoạch thay thế hoặc thuê Bên xử lý phụ mới bằng cách cung cấp thông tin đó cho Bên kiểm soát dữ liệu chậm nhất 14 ngày theo lịch trước sự kiện dự kiến.

7.4. Nếu Bên kiểm soát dữ liệu tiếp tục sử dụng Dịch vụ sau khi Bên xử lý dữ liệu thay thế hoặc thuê Bên xử lý phụ mới và đã được thông báo theo thủ tục nêu tại khoản 7.3 của Thỏa thuận xử lý dữ liệu này, thì được coi là Bên kiểm soát dữ liệu đã đồng ý với những hành động đó của Bên xử lý dữ liệu. Nếu Bên kiểm soát dữ liệu không đồng ý với việc thay thế hoặc sự tham gia của Bên xử lý phụ đó, Bên kiểm soát dữ liệu có quyền đơn phương chấm dứt Thỏa thuận theo thủ tục ngoài tòa án. Trong trường hợp này, việc chấm dứt Thỏa thuận là biện pháp duy nhất mà Bên kiểm soát dữ liệu có thể áp dụng, và Bên xử lý dữ liệu không có nghĩa vụ bồi thường thiệt hại cho Bên kiểm soát dữ liệu.

7.5. Nếu Bên kiểm soát dữ liệu rút lại sự đồng ý chung đối với việc thuê Bên xử lý phụ, Bên xử lý dữ liệu có quyền đơn phương chấm dứt Thỏa thuận theo thủ tục ngoài tòa án. Việc chấm dứt đó được coi là vì lý do chính đáng, và Bên kiểm soát dữ liệu được coi là không phải chịu bất kỳ thiệt hại nào do việc chấm dứt đó.

8. Vi phạm dữ liệu

8.1. Bên xử lý dữ liệu sẽ thông báo cho Bên kiểm soát dữ liệu về mọi Vi phạm dữ liệu ảnh hưởng đến Dữ liệu cá nhân, qua địa chỉ email được ghi trong Đề xuất bán hàng hoặc, nếu không có địa chỉ nào được ghi, qua địa chỉ email của chủ tài khoản của Bên kiểm soát dữ liệu. Thông báo phải được gửi không chậm trễ quá mức, và chậm nhất trong vòng 24 giờ sau khi biết về Vi phạm dữ liệu. Có tính đến bản chất của Dịch vụ được cung cấp, việc xử lý Dữ liệu cá nhân và thông tin hiện có, Bên xử lý dữ liệu sẽ cung cấp cho Bên kiểm soát dữ liệu các thông tin sau: (i) bản chất của Vi phạm dữ liệu, bao gồm, nếu có thể, các nhóm chủ thể dữ liệu liên quan và số lượng gần đúng; (ii) các hậu quả có thể xảy ra của Vi phạm dữ liệu; (iii) các biện pháp mà Bên xử lý dữ liệu đã áp dụng hoặc dự kiến thực hiện để khắc phục Vi phạm dữ liệu, bao gồm, khi phù hợp, các biện pháp

giảm thiểu những hậu quả bất lợi có thể xảy ra; (iv) họ tên đầy đủ và thông tin liên hệ của cán bộ bảo vệ dữ liệu hoặc người liên hệ khác có thể cung cấp thêm thông tin.

8.2. Bên xử lý dữ liệu sẽ ghi lại toàn bộ các Vi phạm dữ liệu, bao gồm các sự kiện liên quan đến Vi phạm dữ liệu, tác động của vi phạm và các biện pháp khắc phục đã thực hiện. Trong các trường hợp được GDPR hoặc luật áp dụng khác quy định, Bên xử lý dữ liệu sẽ cung cấp tài liệu đó cho cơ quan giám sát.

8.3. Có tính đến bản chất của việc xử lý và thông tin mà Bên xử lý dữ liệu có được, Bên xử lý dữ liệu sẽ hỗ trợ Bên kiểm soát dữ liệu bảo đảm tuân thủ các nghĩa vụ theo Điều 33 và 34 GDPR. Bên kiểm soát dữ liệu vẫn chịu trách nhiệm thông báo cho cơ quan giám sát và, khi cần thiết, cho các chủ thể dữ liệu. Trừ trường hợp Vi phạm dữ liệu do Bên xử lý dữ liệu vi phạm các nghĩa vụ theo Thỏa thuận xử lý dữ liệu này, sự hỗ trợ của Bên xử lý dữ liệu vượt quá việc thông báo nêu tại khoản 8.1 có thể phát sinh thêm phí.

9. Chuyển Dữ liệu cá nhân sang quốc gia thứ ba

9.1. Mọi việc chuyển dữ liệu cá nhân sang quốc gia thứ ba (ngoài EU/EEA) do Bên xử lý dữ liệu thực hiện chỉ được diễn ra trên cơ sở chỉ dẫn bằng văn bản của Bên kiểm soát dữ liệu, và luôn phải tuân thủ Chương V GDPR.

9.2. Việc Bên kiểm soát dữ liệu chấp thuận các Bên xử lý phụ được liệt kê trong Phụ lục B cấu thành chỉ dẫn bằng văn bản đối với các việc chuyển dữ liệu mà các Bên xử lý phụ đó thực hiện, như đã mô tả tại đó. Mỗi việc chuyển dữ liệu như vậy phải dựa trên một quyết định về mức độ bảo vệ đầy đủ của Ủy ban châu Âu (bao gồm Khuôn khổ Bảo mật Dữ liệu EU–Hoa Kỳ đối với các bên nhận đã được chứng nhận), các Điều khoản hợp đồng tiêu chuẩn của Ủy ban châu Âu hoặc một công cụ chuyển dữ liệu khác theo Chương V GDPR.

10. Hợp tác

10.1. Có tính đến bản chất của các Dịch vụ được cung cấp, việc xử lý Dữ liệu khách hàng và thông tin hiện có, Bên xử lý dữ liệu sẽ hợp tác với Bên kiểm soát dữ liệu để bảo đảm thực hiện các nghĩa vụ nêu tại Điều 32–36 GDPR. Vì mục đích này, và chỉ trong phạm vi được nêu trong Thỏa thuận xử lý dữ liệu này, Bên xử lý dữ liệu sẽ cung cấp cho Bên kiểm soát dữ liệu các thông tin được yêu cầu, cần thiết để Bên kiểm soát dữ liệu thực hiện đúng các nghĩa vụ theo GDPR.

10.2. Khi loại hình xử lý, đặc biệt là việc sử dụng công nghệ mới, và có tính đến bản chất, phạm vi, bối cảnh và mục đích của việc xử lý, có khả năng dẫn đến rủi ro cao đối với quyền và tự do của các cá nhân, Bên xử lý dữ liệu sẽ hỗ trợ Bên kiểm soát dữ liệu, trước khi xử lý, trong việc đánh giá tác động của các hoạt động xử lý dự kiến đối với việc bảo vệ Dữ liệu cá nhân.

10.3. Nếu chủ thể dữ liệu, cơ quan giám sát hoặc bên thứ ba yêu cầu Bên xử lý dữ liệu cung cấp bất kỳ thông tin nào về Dữ liệu cá nhân đã được xử lý theo quy định của pháp luật, Bên xử lý dữ liệu sẽ chuyển các yêu cầu đó cho Bên kiểm soát dữ liệu mà không chậm trễ quá mức. Bên xử lý dữ liệu cam kết hỗ trợ Bên kiểm soát dữ liệu ở mức cần thiết để phản hồi các yêu cầu của chủ thể dữ liệu, cơ quan giám sát hoặc bên thứ ba, và thực hiện các nghĩa vụ của Bên kiểm soát dữ liệu liên quan đến việc thực thi quyền của chủ thể dữ liệu, bao gồm nhưng không giới hạn ở quyền đính chính và xóa dữ liệu cá nhân, quyền di chuyển dữ liệu cá nhân, quyền phản đối và hạn chế việc xử lý. Bên xử lý dữ liệu sẽ bảo đảm thông tin mà mình nắm giữ được cung cấp trong thời hạn do pháp luật quy định.

11. Nghĩa vụ của Bên kiểm soát dữ liệu

11.1. Bên kiểm soát dữ liệu sẽ tự quyết định, theo đánh giá và trách nhiệm riêng, các loại Dữ liệu cá nhân và nhóm chủ thể dữ liệu được cung cấp cho Bên xử lý dữ liệu, và chỉ cung cấp cho Bên xử lý dữ liệu những Dữ liệu cá nhân cần thiết để Bên xử lý dữ liệu cung cấp Dịch vụ một cách đúng đắn. Bên kiểm soát dữ liệu chịu mọi rủi ro liên quan, bao gồm rủi ro Bên xử lý dữ liệu nhận được nhiều Dữ liệu cá nhân hơn mức cần thiết.

11.2. Bên kiểm soát dữ liệu cam kết và bảo đảm rằng mình đã có, và sẽ duy trì trong suốt thời hạn của Thỏa thuận, mọi giấy phép và ủy quyền cần thiết để cung cấp Dữ liệu cá nhân cho Bên xử lý dữ liệu và thuê Bên xử lý dữ liệu xử lý Dữ liệu cá nhân theo Thỏa thuận.

12. Xóa và trả lại Dữ liệu cá nhân

12.1. Khi Thỏa thuận hoặc Thỏa thuận xử lý dữ liệu này chấm dứt, theo lựa chọn của Bên kiểm soát dữ liệu, Bên xử lý dữ liệu sẽ xóa toàn bộ Dữ liệu cá nhân đã được xử lý thay mặt Bên kiểm soát dữ liệu, hoặc trả lại toàn bộ Dữ liệu cá nhân cho Bên kiểm soát dữ liệu (Bên kiểm soát dữ liệu có thể xuất dữ liệu của mình từ Dịch vụ bất cứ lúc nào), và xóa mọi bản sao hiện có, đồng thời xác nhận với Bên kiểm soát dữ liệu rằng mình đã thực hiện việc đó, trừ khi luật của Liên minh hoặc của Quốc gia thành viên yêu cầu lưu giữ Dữ liệu cá nhân. Các bản sao trong bản sao lưu sẽ được xóa khi bản sao lưu hết hạn theo chu kỳ thông thường và không được sử dụng cho bất kỳ mục đích nào khác trong thời gian đó.

13. Trách nhiệm pháp lý

13.1. Bất kể Bên kiểm soát dữ liệu phải chịu thiệt hại nào, toàn bộ trách nhiệm của Bên xử lý dữ liệu theo Thỏa thuận xử lý dữ liệu này được giới hạn như sau: tổng trách nhiệm của Bên xử lý dữ liệu và bất kỳ nhà cung cấp nào của Bên xử lý dữ liệu đối với mọi yêu cầu bồi thường phát sinh theo hoặc liên quan đến Thỏa thuận xử lý dữ liệu này sẽ không vượt quá số tiền mà Bên kiểm soát dữ liệu đã thực trả cho Bên xử lý dữ liệu đối với Dịch vụ trong mười hai (12) tháng trước ngày xảy ra sự kiện làm phát sinh yêu cầu bồi thường. Trong phạm vi tối đa mà luật hiện hành cho phép, Bên xử lý dữ liệu hoặc các nhà cung cấp của Bên xử lý dữ liệu trong mọi trường hợp đều không chịu trách nhiệm đối với bất kỳ thiệt hại đặc biệt, ngẫu nhiên, gián tiếp hoặc hệ quả nào (bao gồm nhưng không giới hạn ở thiệt hại về lợi nhuận, dữ liệu hoặc thông tin khác, gián đoạn kinh doanh, thương tích cá nhân, mất quyền riêng tư), ngay cả khi Bên xử lý dữ liệu hoặc một nhà cung cấp đã được thông báo về khả năng xảy ra các thiệt hại đó, và ngay cả khi biện pháp khắc phục không đạt được mục đích thiết yếu của nó.

13.2. Các giới hạn tại khoản 13.1 chỉ áp dụng giữa các bên. Các giới hạn này không áp dụng đối với trách nhiệm không thể bị giới hạn theo luật hiện hành và không ảnh hưởng đến quyền của chủ thể dữ liệu theo Điều 82 GDPR.

14. Hiệu lực và chấm dứt

14.1. Thỏa thuận xử lý dữ liệu này có hiệu lực kể từ khi Thỏa thuận có hiệu lực và tiếp tục có hiệu lực trong suốt thời gian Thỏa thuận còn hiệu lực. Các nghĩa vụ của Bên xử lý dữ liệu tiếp tục tồn tại trong suốt thời gian Bên xử lý dữ liệu xử lý Dữ liệu cá nhân thay mặt Bên kiểm soát dữ liệu.

15. Điều khoản cuối cùng

15.1. Bên xử lý dữ liệu sẽ thông báo về mọi thay đổi dự kiến đối với Thỏa thuận xử lý dữ liệu này ít nhất 30 ngày trước khi thay đổi có hiệu lực. Nếu Bên kiểm soát dữ liệu tiếp tục sử dụng Dịch vụ sau khi các thay đổi đối với Thỏa thuận xử lý dữ liệu được công bố, thì được coi là Bên kiểm soát dữ liệu đồng ý với các thay đổi đó. Nếu Bên kiểm soát dữ liệu không đồng ý với các thay đổi, Bên kiểm soát dữ liệu sẽ không thể sử dụng Dịch vụ và có quyền chấm dứt Thỏa thuận.

15.2. Trong trường hợp có mâu thuẫn giữa Thỏa thuận xử lý dữ liệu này và Thỏa thuận, Thỏa thuận xử lý dữ liệu này được ưu tiên áp dụng đối với việc xử lý Dữ liệu cá nhân.

15.3. Thỏa thuận xử lý dữ liệu này chịu sự điều chỉnh của cùng luật, và các tranh chấp được giải quyết theo cùng cách, như quy định trong Thỏa thuận.

15.4. Các phụ lục:

- Phụ lục A: Chi tiết về việc xử lý Dữ liệu cá nhân;
- Phụ lục B: Các Bên xử lý phụ đã được chấp thuận;
- Phụ lục C: Biện pháp kỹ thuật và tổ chức

Phụ lục A – Chi tiết về việc xử lý Dữ liệu cá nhân

Đối tượng và thời hạn	Việc xử lý Dữ liệu cá nhân liên quan đến Dịch vụ trong suốt thời hạn của Thỏa thuận, và sau đó cho đến khi Dữ liệu cá nhân bị xóa hoặc được trả lại theo khoản 12.
Bản chất của việc xử lý	Lưu trữ và lưu giữ dữ liệu; thu thập Dữ liệu cá nhân thông qua các chiến dịch và biểu mẫu của Bên kiểm soát dữ liệu; hiển thị, xuất và xóa trong Dịch vụ; gửi email và tin nhắn cho người tham gia mà Bên kiểm soát dữ liệu thiết lập (ví dụ: xác nhận, mã và thông báo trúng thưởng); chuyển dữ liệu sang hệ thống riêng của Bên kiểm soát dữ liệu thông qua các tích hợp, webhook và API theo chỉ dẫn của Bên kiểm soát dữ liệu; hỗ trợ và xử lý lỗi.
Mục đích xử lý Dữ liệu cá nhân	Để Bên kiểm soát dữ liệu có thể sử dụng Dịch vụ của Bên xử lý dữ liệu như đã thỏa thuận trong Thỏa thuận
Hoạt động xử lý Dữ liệu cá nhân	Thu thập và lưu trữ Dữ liệu khách hàng, bao gồm Dữ liệu cá nhân được cung cấp khi sử dụng Dịch vụ
Các loại Dữ liệu cá nhân	Tên, họ, email, địa chỉ IP và vị trí gần đúng suy ra từ địa chỉ đó, thời điểm đăng ký (created at) và các dữ liệu bổ sung như ngày sinh và số điện thoại (nếu Khách hàng thu thập). Tùy theo cách Bên kiểm soát dữ liệu thiết lập chiến dịch, còn có câu trả lời cho các câu hỏi trong chiến dịch, kết quả trò chơi và giải thưởng đã trúng, mã, bản ghi sự đồng ý, các tệp do người tham gia tải lên (ví dụ: hình ảnh) và dữ liệu kỹ thuật như thông tin trình duyệt và thiết bị.
Dữ liệu thuộc các loại đặc biệt	Không dự kiến. Bên kiểm soát dữ liệu không được thu thập qua Dịch vụ các loại dữ liệu cá nhân đặc biệt (Điều 9 GDPR) hoặc dữ liệu về án tích hình sự (Điều 10 GDPR), trừ khi có thỏa thuận bằng văn bản.

Nhóm chủ thể dữ liệu	Người tham gia các chiến dịch của Bên kiểm soát dữ liệu (Khách hàng), khách truy cập các chiến dịch của Bên kiểm soát dữ liệu nhưng không đăng ký (địa chỉ IP, vị trí gần đúng và thông tin trình duyệt), và người dùng Dịch vụ của Bên kiểm soát dữ liệu trong phạm vi dữ liệu của họ được xử lý thay mặt Bên kiểm soát dữ liệu.
Địa điểm xử lý Dữ liệu cá nhân	Dữ liệu cá nhân được xử lý tại cơ sở của Bên xử lý dữ liệu và trên các máy chủ ảo đặt tại Liên minh châu Âu, cũng như bởi các Bên xử lý phụ được liệt kê trong Phụ lục B tại các địa điểm được nêu ở đó.
Thời lượng xử lý/Thời hạn lưu trữ	Do Bên kiểm soát dữ liệu thiết lập trong Dịch vụ. Phù hợp với khoản 9.4 của Điều khoản và điều kiện, Bên xử lý dữ liệu có thể xóa Dữ liệu cá nhân đã cũ hơn ba (3) năm.

Phụ lục B – Các Bên xử lý phụ đã được chấp thuận

Tại thời điểm ký kết Thỏa thuận xử lý dữ liệu này, Bên kiểm soát dữ liệu chấp thuận việc thuê các Bên xử lý phụ được liệt kê dưới đây. Các việc chuyển dữ liệu ra ngoài EU/EEA dựa trên Khuôn khổ Bảo mật Dữ liệu EU–Hoa Kỳ khi bên nhận đã được chứng nhận, hoặc dựa trên các Điều khoản hợp đồng tiêu chuẩn của Ủy ban châu Âu (khoản 9.2).

Bên xử lý phụ	Mô tả việc xử lý	Địa điểm xử lý
Amazon Web Services EMEA SARL, Luxembourg (AWS)	Lưu trữ Dịch vụ: máy chủ, cơ sở dữ liệu, lưu trữ tệp, bản sao lưu, bộ nhớ đệm và nhật ký	Liên minh châu Âu (Stockholm, Thụy Điển). Nội dung được phân phối qua mạng Amazon CloudFront, có thể xử lý lưu lượng tại các điểm biên ngoài EU/EEA.
ClickHouse, Inc. (ClickHouse Cloud)	Cơ sở dữ liệu phân tích cho thống kê chiến dịch, chẳng hạn như lượt truy cập, lượt tham gia và lượt đăng ký, bao gồm địa chỉ IP và thông tin trình duyệt	Liên minh châu Âu (Frankfurt, Đức), được lưu trữ trên AWS.
Mailgun Technologies, Inc. (thuộc Sinch)	Gửi email mà Bên kiểm soát dữ liệu thiết lập cho người tham gia, chẳng hạn như xác nhận, mã và thông báo trúng thưởng, bao gồm việc gửi, mở và nhấp khi tính năng theo dõi được bật	Liên minh châu Âu (khu vực EU cho dữ liệu thư); thông tin tài khoản hạn chế có thể được xử lý trên toàn cầu.
ip-api.com	Tra cứu vị trí gần đúng của địa chỉ IP người tham gia và phát hiện lưu lượng từ proxy và trung tâm dữ liệu, nhằm ngăn chặn gian lận và bot	Romania (EU); không thể loại trừ việc xử lý hoặc chuyển dữ liệu ra ngoài EU/EEA.
Google (Gemini API)	Các tính năng AI trong Dịch vụ, chẳng hạn như trợ lý AI, dịch thuật và tạo văn bản. Dữ liệu người tham gia chỉ được gửi dưới dạng đã được giả danh hóa hoặc tổng hợp (ví dụ: chữ cái đầu, tên miền email và thời điểm đăng ký), trừ khi người dùng của Bên kiểm soát dữ liệu tự nhập dữ liệu đó	Hoa Kỳ và có thể là các quốc gia khác, tùy thuộc vào điểm cuối API và cấu hình xử lý.

Bên xử lý phụ	Mô tả việc xử lý	Địa điểm xử lý
Functional Software, Inc. (Sentry)	Giám sát lỗi và ghi lại phiên làm việc của Dịch vụ, nhằm tìm và sửa lỗi. Báo cáo có thể bao gồm mã nhận dạng nội bộ của người dùng và tài khoản cũng như dữ liệu kỹ thuật về trình duyệt của người dùng của Bên kiểm soát dữ liệu. Văn bản trong bản ghi phiên được che giấu	Liên minh châu Âu (Đức, khu vực EU của Sentry).
Cloudflare, Inc. (Turnstile)	Bảo vệ chống bot trên biểu mẫu chiến dịch, chỉ khi Bên kiểm soát dữ liệu bật tính năng này cho một chiến dịch. Nhận địa chỉ IP và tín hiệu trình duyệt của người tham gia	Mạng toàn cầu; việc xử lý có thể diễn ra ngoài EU/EEA.
Features & Labels, Inc. (fal.ai)	Tạo và chỉnh sửa hình ảnh bằng AI, xóa nền và lồng tiếng trong Dịch vụ. Nhận các lời nhắc và hình ảnh do người dùng của Bên kiểm soát dữ liệu gửi lên	Hoa Kỳ.
Adressevælger (adressevaelger.dk)	Gợi ý địa chỉ trên biểu mẫu chiến dịch, chỉ khi Bên kiểm soát dữ liệu bật tính năng này cho một chiến dịch. Nhận nội dung địa chỉ người tham gia nhập và địa chỉ IP của người tham gia	Đan Mạch (EU).

Phụ lục C – Biện pháp kỹ thuật và tổ chức

Bên xử lý dữ liệu duy trì hệ thống quản lý an toàn thông tin được chứng nhận theo ISO/IEC 27001:2022 bởi Bureau Veritas (số chứng nhận FIHSK27150F). Các biện pháp bao gồm:

- **An ninh lưu trữ và vật lý:** toàn bộ dữ liệu khách hàng được lưu trữ tại các trung tâm dữ liệu của Amazon Web Services (AWS) trong Liên minh châu Âu. Bên xử lý dữ liệu không vận hành máy chủ riêng; an ninh vật lý và môi trường do AWS đảm nhiệm, và AWS được chứng nhận ISO 27001 và SOC 2.
- **An ninh mạng:** máy chủ và cơ sở dữ liệu chạy trong một mạng riêng (Amazon VPC) không thể truy cập từ internet. Chỉ bộ cân bằng tải và mạng phân phối nội dung là công khai, được bảo vệ bởi tường lửa ứng dụng web (AWS WAF) và cơ chế chống tấn công DDoS.
- **Mã hóa:** toàn bộ lưu lượng được mã hóa bằng TLS (HTTPS). Cơ sở dữ liệu, tệp và bản sao lưu được mã hóa khi lưu trữ bằng AES-256. Thông tin xác thực của các tích hợp còn được mã hóa ở cấp ứng dụng. Mật khẩu được băm và thêm muối bằng bcrypt.
- **Kiểm soát truy cập:** kiểm soát truy cập theo vai trò đối với người dùng của Khách hàng, xác thực hai yếu tố và đăng nhập một lần bằng Google, hết thời gian phiên làm việc, và giới hạn số lần thử đăng nhập. Quyền truy cập của nhân viên tuân theo nguyên tắc đặc quyền tối thiểu và nhu cầu cần biết, sử dụng tài khoản riêng biệt và xác thực đa yếu tố khi có thể, được xem xét ít nhất mỗi năm một lần, và bị thu hồi khi nhân viên nghỉ việc.
- **Phân tách:** dữ liệu khách hàng được phân tách về mặt logic theo từng tài khoản (cách ly người thuê), và mọi yêu cầu đều được ủy quyền.

- **Ghi nhật ký và giám sát:** mọi thay đổi trong hạ tầng được ghi lại trong một nhật ký kiểm toán cho phép phát hiện mọi hành vi can thiệp, nhật ký ứng dụng được thu thập tập trung, nền tảng được giám sát suốt ngày đêm, và Khách hàng có thể xem hoạt động của người dùng trong nhật ký hoạt động.
- **Tính sẵn sàng và khả năng phục hồi:** sao lưu được mã hóa hằng ngày, lưu giữ tối thiểu bảy ngày và được lưu trữ tách biệt với môi trường sản xuất; việc khôi phục dữ liệu được kiểm tra ít nhất mỗi năm một lần; các kế hoạch duy trì hoạt động kinh doanh và khôi phục sau thảm họa được xem xét và diễn tập hằng năm.
- **Quản lý sự cố:** quy trình được lập thành văn bản để báo cáo, đánh giá, ngăn chặn, phân tích và theo dõi các sự cố an ninh, bao gồm việc thông báo về Vi phạm dữ liệu theo khoản 8.
- **Phát triển và vận hành an toàn:** máy chủ chạy dưới dạng container bất biến, không có truy cập SSH và không bao giờ được thay đổi thủ công; các thay đổi được kiểm thử trước khi phát hành.
- **Con người:** nhân viên bị ràng buộc bởi nghĩa vụ bảo mật và được đào tạo nhận thức an toàn thông tin như một phần của hệ thống quản lý an toàn thông tin. Các đối tác có quyền truy cập vào hạ tầng cũng được chứng nhận ISO 27001 và chỉ nhận quyền truy cập cần thiết cho công việc của họ.
- **Tối thiểu hóa dữ liệu và công cụ xóa dữ liệu:** Bên kiểm soát dữ liệu quyết định mỗi chiến dịch thu thập dữ liệu nào, và có thể xuất, xóa hoặc tự động xóa dữ liệu người tham gia.