

Chính sách bảo mật và quyền riêng tư của T5Research

Thực hiện bởi:

CÔNG TY CỔ PHẦN NGHIÊN CỨU MẶT TRỜI THÁNG NĂM (T5RESEARCH)

9/6 Nguyễn Tuân, Phường 3, Quận Gò Vấp, Thành phố Hồ Chí Minh

Nội dung

1.Mục đích/mục tiêu.....	3
2.Phạm vi hiệu lực.....	3
3.Nội dung chính sách.....	3
3.1.Quyền và Nghĩa vụ của chủ thể dữ liệu	3
3.1.1.Quyền của chủ thể dữ liệu	3
3.1.2.Nghĩa vụ của chủ thể dữ liệu.....	4
3.2.Những dữ liệu chúng tôi thu thập, lưu trữ và xử lý.....	5
3.2.1.Các hình thức T5R thu thập thông tin cá nhân.....	5
3.2.2.Những dữ liệu chúng tôi thu thập, lưu trữ và xử lý	5
3.2.3.Cookies là gì và cách chúng được sử dụng.....	5
3.3.Xử lý dữ liệu cá nhân.....	Error! Bookmark not defined.
3.4.Chuyển dữ liệu ra nước ngoài	6
3.5.Chia sẻ dữ liệu.....	6
3.5.1.Đối với khách hàng.....	7
3.5.2.Đối với nhân viên.....	7
3.5.3.Đối với cộng tác viên.....	Error! Bookmark not defined.
3.5.4.Đối với cộng tác viên.....	7
3.6.Lưu trữ, xóa, hủy dữ liệu.....	7
4.Dữ liệu trẻ em.....	8
5.Xóa người dùng	9
6.Các loại xóa bằng câu hỏi.....	9
7.Từ chối trách nhiệm	10
8. Xử lý vi phạm	10
8.1. Vi phạm bảo mật dữ liệu là gì?	10
8.2. Khi nào cần thông báo vi phạm	10
8.3. Ai làm gì khi dữ liệu cá nhân bị xâm phạm?	10
8.4. Phân loại vi phạm.....	11
8.5. Đánh giá phạm vi và tác động.....	11
8.6. Xem xét và giám sát	11
9.Liên hệ.....	11

1. Mục đích/mục tiêu

T5Research cam kết bảo vệ dữ liệu chung của các bên liên quan một cách an toàn và bảo mật, tuân thủ nghiêm ngặt Quy định Bảo vệ Dữ liệu Chung Châu Âu (GDPR) từ 2019 và Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân của Chính phủ Việt Nam. Chúng tôi hiểu rằng dữ liệu chung và cá nhân rất quan trọng. Chúng tôi sẽ luôn nỗ lực để giữ an toàn cho dữ liệu, và tuyệt đối không bao giờ trao đổi hoặc bán dữ liệu cá nhân cho một bên thứ ba nào khác trong bất kỳ trường hợp nào.

Chính sách của chúng tôi khác biệt thông qua việc áp dụng công nghệ và quy trình xử lý dữ liệu chặt chẽ, giảm thiểu tối đa việc tiếp xúc và các thao tác thủ công của con người đối với các loại dữ liệu nhạy cảm, dữ liệu định danh; từ đó, hạn chế nguy cơ sai sót và vi phạm có thể xảy ra. Chúng tôi thường xuyên cập nhật chính sách theo các quy định của Châu Âu và chính phủ hiện hành và áp dụng cho toàn bộ thành viên trong công ty, cộng tác viên, đối tác, chủ thể dữ liệu, bên kiểm soát hoặc xử lý dữ liệu nếu có... theo 6 điểm chính bên dưới.

2. Phạm vi hiệu lực

Chính sách này áp dụng cho tất cả các hoạt động liên quan đến thông tin T5Research, cho dù được thực hiện bởi nhân viên của T5Research hay đối tác. Điều này bao gồm tất cả dữ liệu về nhân sự, dữ liệu về các vấn đề tài chính, tất cả dữ liệu đóng góp cho việc quản lý công ty, dữ liệu sản xuất và dữ liệu khảo sát cũng như thông tin do người khác để lại cho T5Research. Dữ liệu này có thể là thông tin thực tế, hồ sơ, đăng ký, báo cáo, điều kiện tiên quyết để lập kế hoạch hoặc thông tin khác chỉ dành cho sử dụng nội bộ. Chính sách bảo mật thông tin có hiệu lực đối với tất cả nhân viên của T5Research và mọi hoạt động sử dụng tài sản thông tin của T5Research.

3. Nội dung chính sách

3.1. Quyền và Nghĩa vụ của chủ thể dữ liệu

3.1.1. Quyền của chủ thể dữ liệu

Quyền được biết

Chủ thể dữ liệu được biết về hoạt động xử lý dữ liệu cá nhân của mình, trừ trường hợp pháp luật có quy định khác.

Quyền đồng ý

Chủ thể dữ liệu được đồng ý hoặc không đồng ý cho phép xử lý dữ liệu cá nhân của mình. Sự đồng ý rõ ràng và minh bạch thông qua một quy trình được ghi nhận lại của chủ thể dữ liệu được thể hiện như sau:

- Nếu đáp viên trả lời “Đồng ý” sẽ được phép phỏng vấn
- Nếu đáp viên im lặng, “Em nói đi”, “Ừ”, “OK” không được xem là đồng ý phỏng vấn.

Quyền rút lại sự đồng ý

Chủ thể dữ liệu được quyền rút lại sự đồng ý của mình, trừ trường hợp luật pháp có quy định khác.

Quyền xóa dữ liệu

Chủ thể dữ liệu được xóa hoặc yêu cầu xóa dữ liệu cá nhân của mình, trừ trường hợp pháp luật có quy định khác.

Quyền hạn chế xử lý dữ liệu

Chủ thể dữ liệu được yêu cầu hạn chế xử lý dữ liệu cá nhân của mình, trừ trường hợp luật pháp có quy định khác.

Việc hạn chế xử lý dữ liệu được thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu, với toàn bộ dữ liệu cá nhân mà chủ thể dữ liệu yêu cầu hạn chế, trừ trường hợp pháp luật có quy định khác.

Quyền cung cấp dữ liệu

Chủ thể dữ liệu được yêu cầu bên Kiểm soát dữ liệu cá nhân, bên Kiểm soát và xử lý dữ liệu cá nhân cung cấp cho bản thân dữ liệu cá nhân của mình, trừ trường hợp luật pháp có quy định khác.

Quyền phản đối xử lý dữ liệu

Chủ thể dữ liệu được phản đối bên Kiểm soát dữ liệu cá nhân, bên Kiểm soát và xử lý dữ liệu cá nhân xử lý dữ liệu cá nhân của mình nhằm ngăn chặn hoặc hạn chế tiết lộ dữ liệu cá nhân hoặc sử dụng cho mục đích quảng cáo, tiếp thị, trừ trường hợp luật pháp có quy định khác.

Bên Kiểm soát dữ liệu cá nhân, bên Kiểm soát và xử lý dữ liệu cá nhân thực hiện yêu cầu của chủ thể dữ liệu trong 72 giờ sau khi nhận được yêu cầu, trừ trường hợp luật pháp quy định khác.

Quyền khiếu nại, tố cáo, khởi kiện

Chủ thể dữ liệu có quyền khiếu nại, tố cáo hoặc khởi kiện theo quy định của pháp luật.

Quyền yêu cầu bồi thường thiệt hại

Chủ thể dữ liệu có quyền yêu cầu bồi thường thiệt hại theo quy định của pháp luật khi xảy ra vi phạm quy định về bảo vệ dữ liệu cá nhân của mình, trừ trường hợp các bên có thỏa thuận khác hoặc luật có quy định khác.

Quyền tự bảo vệ

Chủ thể dữ liệu có quyền tự bảo vệ theo quy định của Bộ luật Dân sự, luật khác có liên quan và Nghị định này, hoặc yêu cầu cơ quan, tổ chức có thẩm quyền thực hiện các phương thức bảo vệ quyền dân sự theo quy định tại Điều 11 Bộ luật Dân sự.

3.1.2. Nghĩa vụ của chủ thể dữ liệu

- Tự bảo vệ dữ liệu cá nhân của mình, yêu cầu các tổ chức, cá nhân khác có liên quan bảo vệ dữ liệu cá nhân của mình.
- Tôn trọng, bảo vệ dữ liệu cá nhân của người khác
- Cung cấp đầy đủ, chính xác dữ liệu cá nhân khi đồng ý cho phép xử lý dữ liệu
- Tham gia tuyên truyền, phổ biến kỹ năng bảo vệ dữ liệu cá nhân

- Thực hiện quy định của pháp luật về bảo vệ dữ liệu cá nhân và tham gia phòng, chống các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân
- Thực hiện quy định của pháp luật về bảo vệ dữ liệu cá nhân và tham gia phòng chống các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân
- Thông báo ngay với chúng tôi nếu phát hiện, nghi ngờ dữ liệu cá nhân của bản thân bị lộ hoặc bất kỳ vi phạm nào về bảo vệ dữ liệu cá nhân theo các điều khoản điều kiện này mà dữ liệu cá nhân có thể nhận biết được.
- Thường xuyên kiểm tra trang thông tin của chúng tôi để cập nhật và thực hiện theo bất kỳ thay đổi (nếu có) liên quan đến chính sách bảo vệ dữ liệu cá nhân tại các điều khoản điều kiện này
- Các nghĩa vụ khác theo quy định của pháp luật

3.2. Những dữ liệu chúng tôi thu thập, lưu trữ và xử lý

3.2.1. Các hình thức T5R thu thập thông tin cá nhân

- Phòng vấn viên thu thập qua tổng đài điện thoại có ghi âm
- Chủ thể dữ liệu cung cấp qua mẫu điền thông tin trực tuyến
- Bên Kiểm soát dữ liệu cá nhân cung cấp

3.2.2. Những dữ liệu chúng tôi thu thập, lưu trữ và xử lý

- Thông tin định danh: Họ tên, số điện thoại, email, khu vực, quốc tịch, GPS. Thông tin nhận dạng cá nhân như tên, e-mail, địa chỉ và số điện thoại sẽ không bao giờ được chuyển cho khách hàng hoặc bên thứ ba của chúng tôi mà không có sự đồng ý của bạn.
 - Nhân khẩu học: giới tính, thu nhập, tình trạng hôn nhân, nghề nghiệp, lĩnh vực, thói quen, hành vi mua sắm, sở thích, tôn giáo, v.v
 - Thông tin sử dụng sản phẩm dịch vụ, quan điểm cá nhân
 - Thông tin nhạy cảm: quan điểm chính trị, tôn giáo, thông tin sức khỏe, thông tin tài chính, hành vi phạm tội, v.v
 - Thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, các tổ chức được phép khác.
 - Thông tin quan điểm, ý kiến cá nhân về các chủ đề nghiên cứu. Ý kiến cá nhân của bạn sẽ được sử dụng duy nhất cho mục đích nghiên cứu và được chia sẻ với khách hàng của chúng tôi, các nhóm nghiên cứu nội bộ và các đối tác của chúng tôi và các câu trả lời này luôn được công bố dưới dạng một nhóm chứ không phải của từng cá nhân cho từng câu hỏi.
 - Bản ghi âm cuộc gọi thành công và không thành công.

Hệ thống T5Research sở hữu khả năng phân loại dữ liệu nhạy cảm hiệu quả, giúp doanh nghiệp có thể dễ dàng thiết lập quy trình xử lý riêng biệt cho từng loại dữ liệu nhạy cảm, đảm bảo tuân thủ các quy định và tối ưu hóa hiệu quả quản lý.

3.2.3. Cookies là gì và cách chúng được sử dụng

Là một phần của việc đưa ra và cung cấp các dịch vụ cá nhân và theo yêu cầu khách hàng, nền tảng T5Research có thể dùng các cookies để lưu trữ và theo dõi thông tin về bạn. Cookies là một lượng nhỏ dữ liệu được gửi tới trình duyệt của bạn từ máy chủ web và được lưu trên đĩa cứng máy tính của bạn.

Bạn có thể chọn bật hoặc tắt một số hoặc tất cả các cookie này. Việc tắt một số cookie có thể ảnh hưởng đến trải nghiệm web của bạn.

Có nhiều loại cookies khác nhau, tuy nhiên, trang web của chúng tôi sử dụng:

- Cookies chức năng – Cookies giúp thực hiện một số chức năng nhất định, chẳng hạn như chia sẻ nội dung của trang web trên nền tảng truyền thông xã hội, thu thập phản hồi và các chức năng khác của bên thứ ba.
- Cookies phân tích – Cookies phân tích được sử dụng để hiểu cách khách truy cập tương tác với trang web. Những cookie này giúp cung cấp thông tin về số lượng khách truy cập, tỷ lệ thoát, nguồn lưu lượng truy cập, v.v.
- Cookies hiệu suất - Cookie hiệu suất được sử dụng để hiểu và phân tích các chỉ số hiệu suất chính của trang web, giúp mang lại trải nghiệm người dùng tốt hơn cho khách truy cập.
- Cookies quảng cáo - Cookie quảng cáo được sử dụng để cung cấp cho khách hàng truy cập quảng cáo tùy chỉnh dựa trên các trang họ đã truy cập trước đó và để phân tích tính hiệu quả của chiến dịch quảng cáo.

3.3. Xử lý dữ liệu cá nhân

Chúng tôi sẽ chỉ thu thập những thông tin cần thiết cho mục đích được quy định cụ thể, rõ ràng và hợp pháp, và đảm bảo thông tin này sẽ không được xử lý theo cách thức không phù hợp với những mục đích như vậy. Cụ thể như sau:

- Cung cấp thông tin về sản phẩm dịch vụ của T5Research: Chúng tôi sử dụng những thông tin bạn cung cấp qua website để gửi thông tin về công ty, liên hệ với bạn khi cần thiết, cá nhân hóa trải nghiệm của bạn trên website, hiển thị nội dung và sản phẩm phù hợp với sở thích của bạn.
- Tiến hành khảo sát nghiên cứu thị trường: Những thông tin bạn đồng ý cung cấp từ các cuộc khảo sát sẽ chỉ được sử dụng duy nhất cho mục đích nghiên cứu và chỉ được sử dụng bởi các nhóm nghiên cứu nội bộ và khách hàng của chúng tôi.
- Kiểm soát chất lượng: Chúng tôi sẽ kiểm định những thông tin thu thập được nhằm đảm bảo tính chính xác và độ tin cậy của dữ liệu nghiên cứu.
- Phân tích dữ liệu và báo cáo: Sau quá trình thu thập và kiểm định chất lượng, dữ liệu sẽ được tổng hợp, phân tích và báo cáo nhằm đưa ra các chiến lược hữu ích.
- Quản lý trải nghiệm khách hàng: phác thảo chân dung khách hàng một cách hoàn chỉnh, thu thập phản hồi, hành vi khách hàng tại mọi điểm chạm với doanh nghiệp và đối thủ cạnh tranh.

3.4. Chuyển dữ liệu ra nước ngoài

Chúng tôi hiểu rằng bạn có thể lo lắng về việc dữ liệu cá nhân của mình bị chuyển ra nước ngoài. Do đó, chúng tôi cam kết 100% dữ liệu cá nhân của bạn đều được lưu trữ và xử lý trong lãnh thổ Việt Nam. Việc này giúp đảm bảo dữ liệu của bạn được bảo vệ bởi luật pháp Việt Nam.

3.5. Chia sẻ dữ liệu

Chúng tôi cam kết bảo vệ quyền riêng tư và sẽ không chia sẻ dữ liệu nếu không có sự đồng ý của chủ thể dữ liệu hoặc người kiểm soát dữ liệu.

3.5.1. Đối với khách hàng

Để đảm bảo an toàn cho thông tin của bạn, T5Research và Khách hàng sẽ ký Thỏa thuận Bảo mật Thông tin (NDA) trước khi bắt đầu bất kỳ dự án nào cam kết bảo mật mọi thông tin trao đổi giữa hai bên trong quá trình hợp tác.

Các thông tin T5R được phép chia sẻ với khách hàng:

- Thông tin được chủ thể dữ liệu cho phép chia sẻ
- Thông tin của Phòng vấn viên: Chỉ cung cấp mã PVV, trình độ, giới tính. Không cung cấp thông tin khác.
- Trạng thái cuộc gọi (call logs)
- Tập tin ghi âm các bài phỏng vấn thành công, có sự đồng ý của chủ thể dữ liệu.

3.5.2. Đối với nhân viên

Tất cả nhân viên T5Research đều tuân thủ quy định bảo mật, bao gồm cả thông tin nội bộ, thông tin về khách hàng và sản phẩm của họ, và thông tin về người tham gia khảo sát. Tham khảo thêm tại file “Chính sách bảo mật dành cho nhân viên”.

3.5.3. Đối với cộng tác viên

Trước khi tham gia, tất cả phỏng vấn viên phải ký thỏa thuận bảo mật thông tin trước khi chúng tôi chia sẻ dữ liệu dự án. Bao gồm:

- Thông tin dự án
- Thông tin khách hàng
- Phương thức, hoạt động và chiến lược kinh doanh của công ty
- Các thông tin dự án, hợp đồng Công ty đã, đang triển khai và sau khi kết thúc
- Các đối tác, khách hàng đã, đang và sẽ thiết lập quan hệ với Công ty
- Tình hình nội bộ, tài chính, nhân sự của Công ty, thông tin tiếp thị, thông tin khách hàng, thông tin kỹ thuật
- Bí mật kinh doanh, bí quyết, nghiên cứu sáng chế, kế hoạch kinh doanh
- Quyền truy cập tài liệu đào training được giới hạn ở chế độ đọc. Chính sửa và tải xuống không được phép bởi chúng tôi đã thiết lập quyền hạn khi chia sẻ dữ liệu.
- Thông tin liên quan đến ID và password vào các hệ thống tại Công ty của cá nhân.
- Bất cứ các thông tin nào khác liên quan đến hoạt động của Công ty và đối tác, khách hàng của Công ty mà cộng tác viên có được trong quá trình làm việc từ bất kỳ nguồn nào
- Các tài liệu được đánh dấu mật.
- Thông tin không được cung cấp nhưng vô tình được biết.

3.5.4. Đối với cộng tác viên

Chúng tôi yêu cầu bên thứ ba tiếp nhận, đảm bảo an toàn, bảo mật đối với dữ liệu được cung cấp, chuyển giao. Chúng tôi chỉ chia sẻ dữ liệu nằm trong phạm vi các thỏa thuận sau:

- Ký thỏa thuận không tiết lộ.
- Thỏa thuận phạm vi xử lý thông tin.

3.6. Lưu trữ, xóa, hủy dữ liệu

Dữ liệu được bảo mật trên nền tảng trực tuyến research.t5r.vn và hệ thống máy chủ đặt tại trung tâm ISP trong phạm vi lãnh thổ Việt Nam. Trong trường hợp máy chủ lưu trữ

thông tin bị hacker tấn công dẫn đến mất dữ liệu, chúng tôi có trách nhiệm thông báo vụ việc cho cơ quan chức năng kiểm tra xử lý kịp thời và thông báo cho bên liên quan được biết.

Với dữ liệu ghi âm, chúng tôi chỉ lưu trữ trong vòng 30 ngày sau khi nghiệm thu dự án. Chủ thể dữ liệu được yêu cầu Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân xóa dữ liệu cá nhân của mình trong các trường hợp sau:

- Nhận thấy không còn cần thiết cho mục đích thu thập đã đồng ý và chấp nhận các thiệt hại có thể xảy ra khi yêu cầu xóa dữ liệu
- Rút lại sự đồng ý
- Phản đối việc xử lý dữ liệu và Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân không có lý do chính đáng để tiếp tục xử lý;
- Dữ liệu cá nhân được xử lý không đúng với mục đích đã đồng ý hoặc việc xử lý dữ liệu cá nhân là vi phạm quy định của pháp luật
- Dữ liệu cá nhân phải xóa theo quy định của pháp luật.

Việc xóa dữ liệu sẽ không áp dụng khi có đề nghị của chủ thể dữ liệu trong các trường hợp:

- Pháp luật quy định không cho phép xóa dữ liệu
- Dữ liệu cá nhân được xử lý bởi cơ quan nhà nước có thẩm quyền với mục đích phục vụ hoạt động của cơ quan nhà nước theo quy định của pháp luật
- Dữ liệu cá nhân đã được công khai theo quy định của pháp luật
- Dữ liệu cá nhân được xử lý nhằm phục vụ yêu cầu pháp lý, nghiên cứu khoa học, thống kê theo quy định của pháp luật
- Trong trường hợp tình trạng khẩn cấp về quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, thảm họa lớn, dịch bệnh nguy hiểm; khi có nguy cơ đe dọa an ninh, quốc phòng nhưng chưa đến mức ban bố tình trạng khẩn cấp; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật
- Ứng phó với tình huống khẩn cấp đe dọa đến tính mạng, sức khỏe hoặc sự an toàn của chủ thể dữ liệu hoặc cá nhân khác.

Trường hợp doanh nghiệp chia, tách, sáp nhập, hợp nhất, giải thể thì dữ liệu cá nhân được chuyển giao theo quy định của pháp luật.

Dữ liệu cá nhân của khách hàng sẽ được lưu trữ cho đến khi có yêu cầu hủy bỏ.

Dữ liệu được xóa về mặt kỹ thuật nếu có bất kỳ yêu cầu từ bên chủ thể dữ liệu hoặc bên kiểm soát dữ liệu về việc từ chối lưu trữ thông tin.

Phòng vấn viên không có quyền truy cập vào hệ thống khi kết thúc ca làm việc.

T5Research không thể cam kết bảo mật một cách tuyệt đối an toàn và chúng tôi không thể chịu trách nhiệm trong trường hợp có sự truy cập trái phép thông tin cá nhân của khách hàng như các trường hợp khách hàng tự ý chia sẻ thông tin với người khác.

4. Dữ liệu trẻ em

Xử lý dữ liệu cá nhân của trẻ em luôn được thực hiện theo nguyên tắc bảo vệ các quyền và vì lợi ích tốt nhất của trẻ em.

Việc xử lý dữ liệu cá nhân của trẻ em phải có sự đồng ý của trẻ em trong trường hợp trẻ em từ đủ 7 tuổi trở lên và có sự đồng ý của cha, mẹ hoặc người giám hộ theo quy định, trừ trường hợp quy định tại Điều 17 Nghị định này. Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân

Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên thứ ba phải xác minh tuổi của trẻ em trước khi xử lý dữ liệu cá nhân của trẻ em

Ngừng xử lý dữ liệu cá nhân của trẻ em, xóa không thể khôi phục hoặc hủy dữ liệu cá nhân của trẻ em trong trường hợp:

- Xử lý dữ liệu không đúng mục đích hoặc đã hoàn thành mục đích xử lý dữ liệu cá nhân được chủ thể dữ liệu đồng ý, trừ trường hợp pháp luật có quy định khác;
- Cha, mẹ hoặc người giám hộ của trẻ em rút lại sự đồng ý cho phép xử lý dữ liệu cá nhân của trẻ em, trừ trường hợp pháp luật có quy định khác;
- Theo yêu cầu của cơ quan chức năng có thẩm quyền khi có đủ căn cứ chứng minh việc xử lý dữ liệu cá nhân gây ảnh hưởng tới quyền và lợi ích hợp pháp của trẻ em, trừ trường hợp pháp luật có quy định khác

5. Xóa người dùng

Xóa vĩnh viễn người dùng: Diễn tả việc xóa người dùng và tất cả dữ liệu câu trả lời bảng hỏi (QAS) và dữ liệu liên quan một cách vĩnh viễn.

Ẩn danh người dùng: Mô tả việc xóa vĩnh viễn tất cả thông tin nhận dạng cá nhân của người dùng và trong tất cả QAS liên quan, nhưng vẫn duy trì mối liên kết giữa các QAS. Sau đó đánh dấu người dùng đó là đã bị vô hiệu hóa. Việc sử dụng tính năng này phụ thuộc vào các câu hỏi được đánh dấu với thiết lập quyền riêng tư GDPR phù hợp.

Gỡ bỏ quyền truy cập người dùng: Mô tả việc xóa vĩnh viễn tất cả thông tin nhận dạng cá nhân của người dùng và tất cả dữ liệu QAS liên quan. Đồng thời, chuyển đổi tất cả dữ liệu QAS liên kết với người dùng bị xóa thành dạng ẩn danh. Cuối cùng, xóa hoàn toàn người dùng đó.

Về mặt kỹ thuật, để thực hiện bất kỳ phương thức xóa nào nêu trên, hệ thống có thể đánh dấu người dùng là "đã vô hiệu hóa" hoặc "đã xóa" tạm thời. Sau đó, việc xóa thực tế sẽ được gom nhóm và thực hiện vào một ngày cụ thể sau này, nhưng thời gian trì hoãn này không được quá 45 ngày. Cách làm này giúp cho phép khôi phục lại tài khoản trong trường hợp xóa nhầm và cũng đơn giản hóa việc quản lý xóa dữ liệu.

6. Các loại xóa bảng câu hỏi

Xóa dữ liệu: Mô tả hành động xóa vĩnh viễn tất cả dữ liệu được thu thập trong một khảo sát (QAS), nhưng không ảnh hưởng đến người dùng, liên kết người dùng hoặc bản thân khảo sát

Xóa khảo sát: Mô tả hành động xóa vĩnh viễn tất cả dữ liệu được thu thập trong một khảo sát (QAS), nhưng không ảnh hưởng đến người dùng hoặc bất kỳ thông tin nào khác của người dùng đó.

Ẩn danh khảo sát: Mô tả hành động xóa vĩnh viễn tất cả thông tin nhận dạng cá nhân trong khảo sát (QAS) và ngắt kết nối khảo sát với người dùng đã điền nó, nhưng vẫn duy trì dữ liệu được thu thập. Điều này có thể được thực hiện bằng cách chuyển đổi thành "Không có người dùng", "Người dùng ẩn danh" hoặc một người dùng ẩn danh mới. Việc sử dụng tính năng này phụ thuộc vào các câu hỏi được đánh dấu với cài đặt quyền riêng tư GDPR phù hợp.

Hủy khảo sát: Mô tả hành động xóa vĩnh viễn bảng câu hỏi và tất cả các khảo sát (QAS) liên quan, bao gồm cả tất cả các khảo sát con của bảng câu hỏi. Ví dụ: nếu người dùng mẫu được nhập làm khảo sát con của bảng câu hỏi, thì chúng cũng sẽ bị xóa. Tương tự với các DCS là khảo sát con của bảng câu hỏi.

7. Từ chối trách nhiệm

Trang mạng của chúng tôi chứa các liên kết đến các trang khác. T5Research không chịu trách nhiệm về nội dung hoặc các quyền riêng tư của những trang này.

8. Xử lý vi phạm

8.1. Vi phạm bảo mật dữ liệu là gì?

Hành vi vi phạm bảo mật dẫn đến việc phá hủy, mất mát, thay đổi, tiết lộ hoặc truy cập trái phép vào dữ liệu cá nhân được truyền, lưu trữ hoặc xử lý một cách vô tình hoặc bất hợp pháp.

Ví dụ: hack hệ thống của chúng tôi hoặc cung cấp thông tin liên hệ của người trả lời cho những người bên ngoài công ty.

8.2. Khi nào cần thông báo vi phạm

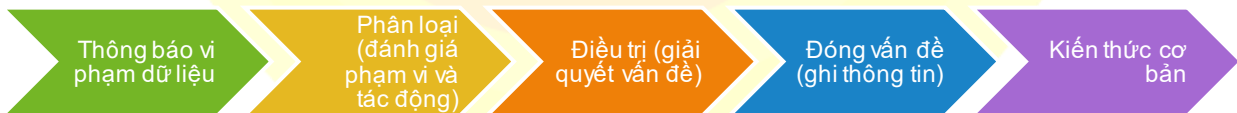
Phải báo cáo các hành vi vi phạm dữ liệu càng sớm càng tốt, nhưng vẫn có các khung thời gian nhất định trước khi chúng tôi phải công bố.

Trong trường hợp dữ liệu của chúng tôi bị vi phạm, T5Research đã được phát hiện 72 giờ sau khi vi phạm để báo cáo việc này cho Cơ quan thanh tra dữ liệu

Nếu có hành vi vi phạm dữ liệu mà chúng tôi nhận được từ khách hàng, chúng tôi thường có 12 giờ sau khi phát hiện hành vi vi phạm để thông báo cho khách hàng về hành vi vi phạm này. Tuy nhiên, trong trường hợp vi phạm dữ liệu mà người khác phải chịu trách nhiệm, thường thì những người đó sẽ thông báo cho Cơ quan kiểm tra dữ liệu rằng chúng tôi là bên xử lý dữ liệu của họ nhưng chúng tôi phải hỗ trợ họ.

8.3. Ai làm gì khi dữ liệu cá nhân bị xâm phạm?

Thực hiện theo 5 bước để giải quyết vấn đề:



Thông thường nhóm xử lý sự cố bảo mật nên báo cáo cho cán bộ phụ trách bảo vệ dữ liệu (DPO) theo quy trình.

Trong trường hợp rủi ro cao đối với quyền và quyền tự do của chủ thể dữ liệu, cán bộ phụ trách bảo vệ dữ liệu (DPO) của bên kiểm soát cần phải thông báo cho Cơ quan Bảo vệ Dữ liệu.

Trong khi DPO đang thông báo cho cơ quan liên quan, điều quan trọng là nhóm xử lý sự cố phải tiếp tục tìm hiểu sâu rộng hai hướng sau:

- Thực hiện tất cả các biện pháp có thể để giảm thiểu rủi ro và ngăn chặn truy cập trái phép hơn nữa
- Tiếp tục tinh chỉnh ước tính ban đầu về số lượng chủ thể dữ liệu bị vi phạm và các loại dữ liệu cá nhân bị vi phạm.

Cán bộ phụ trách bảo vệ dữ liệu (DPO) của bên kiểm soát có thể cần thông báo cho các

chủ thể dữ liệu nếu rủi ro cao đối với quyền và quyền tự do của họ.

Theo hợp đồng, cán bộ phụ trách bảo vệ dữ liệu (DPO) bên xử lý dữ liệu phải thông báo cho bên kiểm soát. Trong trường hợp này, mọi vi phạm dữ liệu cá nhân đều cần được báo cáo cho bên kiểm soát, không có ngoại lệ.

8.4. Phân loại vi phạm

DPO phải hợp tác với nhân viên/nhóm để xác định mức độ vi phạm dữ liệu theo hai thông số sau:

- Tác động: gây thiệt hại cho doanh nghiệp (hợp đồng với khách hàng, quan trọng là vi phạm dữ liệu)
- Tính khẩn cấp: tốc độ mà tổ chức cần để khắc phục vi phạm dữ liệu

Khẩn cấp/Tác động	Cao	Trung bình	Thấp
Cao	1	2	3
Trung bình	2	3	4
Thấp	3	4	5

8.5. Đánh giá phạm vi và tác động

Xác định mức độ tác động và phạm vi vi phạm dữ liệu cá nhân

- Loại vi phạm bảo mật (sẽ có rủi ro lớn hơn nếu dữ liệu được gửi cho người ngoài so với khi dữ liệu bị xóa)
- Bản chất và mức độ thông tin (thông tin sức khỏe có nguy cơ cao hơn thói quen ăn uống)
- Nguy cơ chủ thể dữ liệu bị nhận dạng
- Hậu quả của việc vi phạm có thể xảy ra đối với chủ thể dữ liệu
- Liệu hành vi vi phạm có bao gồm các đối tượng dữ liệu đặc biệt hay không (ví dụ: trẻ em hoặc đặc biệt dễ bị tổn thương)
- Số lượng người bị ảnh hưởng.

8.6. Xem xét và giám sát

Sau khi vi phạm dữ liệu cá nhân đã được ngăn chặn, tiến hành xem xét các biện pháp hiện có và khám phá những cách có thể để tăng cường các biện pháp này nhằm ngăn chặn vi phạm tương tự tái diễn. Tất cả các biện pháp được xác định như vậy cần được giám sát để đảm bảo rằng các biện pháp đó được thực hiện thỏa đáng.

Tất cả thông tin được tạo ra trong quá trình xử lý vi phạm dữ liệu đều rất quan trọng đối với hành vi vi phạm dữ liệu tương tự có thể xảy ra trong tương lai cũng như để thu thập bằng chứng. Nếu sự cố xảy ra lần nữa trong tương lai, chúng ta chỉ cần tham khảo cơ sở kiến thức là sẽ có giải pháp hoàn hảo mà không cần tốn thời gian.

Luôn ghi nhật ký hành động và ghi nhật ký vi phạm dữ liệu.

9. Liên hệ

Nếu bạn có bất kỳ thắc mắc hay lo ngại về chính sách bảo mật và quyền riêng tư của chúng tôi, xin vui lòng liên hệ với chúng tôi qua:

- Số điện thoại: +84 28 39941168
- Email: sale@t5r.vn



- Địa chỉ gửi thư: 9/6 Nguyễn Tuân, Phường 3, Quận Gò Vấp, Thành phố Hồ Chí Minh, Việt Nam.

