Sổ tay nhân viên

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

Cẩm nang quy định về Bảo vệ Dữ liệu chung

Chúng tôi có các quy trình chặt chẽ để bảo vệ thông tin cá nhân của bạn, tuân thủ theo luật pháp và thỏa thuận với khách hàng.
Tài liệu này này cung cấp thông tin về cách thức xử lý thông tin cá nhân của bạn, cũng như các bước cần thực hiện khi phát hiện vấn đề. Quy định về Bảo vệ Dữ liệu Chung (GDPR) được thông qua nhằm đảm bảo thông tin cá nhân của bạn được sử dụng cho mục đích cụ thể và chính đáng.
Những thay đổi đối với cẩm nang bảo mật thông tin phải thông qua và được hội đồng quản trị phê duyệt. Những thay đổi về quy trình hoạt động có thể được thực hiện ở mỗi bộ phận.

Thông tin cá nhân là gì?

Thông tin cá nhân được phân thành 4 loại, trong đó dữ liệu có thể thuộc nhiều hơn 1 loại.

- Thông tin nhận dạng cá nhân: Bất kỳ dạng dữ liệu nào có thể được sử dụng để nhận dạng một cá nhân. Ví dụ: Tên, e-mail, hình ảnh, địa chỉ IP, hoặc mã định danh từ cơ sở dữ liệu nào đó.
- Thông tin nhạy cảm. Đây là danh sách thông tin cụ thể được đánh dấu là nhạy cảm:
  - Sức khỏe
  - Thành viên công đoàn
  - Nguồn gốc chủng tộc hoặc dân tộc
  - Quan điểm chính trị, tôn giáo
  - Khuynh hướng tình dục
  - Dữ liệu di truyền và sinh trắc học để nhận dạng cá nhân
- Thông tin đặc biệt: Đây là những thông tin quan trọng hơn so với thông tin cá nhân thông thường, cần được bảo mật ở mức độ cao hơn. Các ví dụ bao gồm số định danh cá nhân (CMT/CCCD), mã số thuế hoặc các mã định dạng khác do Chính phủ cấp, cũng như tiền án tiền sự (nếu có). Mặc dù đây không phải là thông tin quá nhạy cảm, nhưng vẫn cần được bảo vệ chặt chẽ.
- Dữ liệu cá nhân: bất kỳ loại dữ liệu nào khi được kết hợp với “Thông tin nhận dạng cá nhân”, thì dữ liệu đó sẽ trở thành dữ liệu cá nhân.

Nếu dữ liệu được kết hợp không thể nhận dạng một người thì dữ liệu đó không phải là thông tin cá nhân, nghĩa là dữ liệu được ẩn danh hoàn toàn. Nếu dữ liệu vẫn chứa bất kỳ loại ID nào, ngay cả khi người nhận dữ liệu không có quyền truy cập vào cơ sở dữ liệu chứa ID đó thì dữ liệu đó vẫn là thông tin cá nhân, mặc dù hiện tại chúng được gọi là dữ liệu ẩn danh một phần.
Ngoài ra, GDPR còn chứa các yêu cầu nghiêm ngặt rằng bất kỳ lúc nào, "bên sở hữu" dữ liệu cũng phải xác định được:

- Bên bảo vệ dữ liệu (Bên kiểm soát): Bên kiểm soát dữ liệu chịu trách nhiệm về việc xử lý thông tin cá nhân theo quy định của pháp luật và các quy trình riêng của họ.
- Bên xử lý dữ liệu (Nhà cung cấp): Nhà cung cấp dữ liệu không có quyền truy cập vào thông tin cá nhân trừ khi Bên kiểm soát dữ liệu cho phép.

Chính sách truy cập thông tin cá nhân chung

- Không được phép đọc, truy cập hoặc thay đổi bất kỳ thông tin cá nhân nào mà không có yêu cầu cụ thể để thực hiện việc đó.

- Nếu bạn phát hiện mình được cấp quyền truy cập vào bất kỳ thông tin cá nhân, nhưng nhiệm vụ hiện tại không yêu cầu phải xem thông tin đó, thì bạn nên liên hệ với quản lý gần nhất.
- Nếu bạn phát hiện bất kỳ ai, kể cả chính bạn, có quyền truy cập hoặc thay đổi bất kỳ thông tin cá nhân nào mà họ không được phép thực hiện hoặc xảy ra bất kỳ rò rỉ nào khác, bạn phải báo cáo ngay lập tức cho Giám đốc Công nghệ (CTO) hiện tại là Dennis Haney Dennis@maysunshine.vn.
- Việc cung cấp hoặc cho phép truy cập vào bất kỳ thông tin cá nhân nào bên ngoài văn phòng của T5Research chỉ được thực hiện với các nhà thầu phụ được phê duyệt trước, chẳng hạn như MaySunshine, và chỉ khi có nhiệm vụ yêu cầu điều đó.
- Các tập tin chứa thông tin cá nhân PHẢI được mã hóa với một mật khẩu riêng biệt, và mọi phiên bản chưa mã hóa của tập tin phải bị xóa bỏ. Mật khẩu phải được lưu trữ ở một vị trí riêng biệt so với tập tin. Ví dụ: nếu tập tin được gửi qua email, thì mật khẩu sẽ được trao đổi qua tin nhắn SMS.
- Khi làm việc với dữ liệu cá nhân, bạn phải tuân theo các thủ tục được quy định trong mọi chính sách, hướng dẫn hoặc sổ tay liên quan.

Tạo tài khoản phỏng vấn mới

- Kiểm tra yêu cầu tạo Thành viên phỏng vấn mới: Phải là Giám sát viên hoặc Thành viên hội đồng quản trị
- Kiểm tra với Người phỏng vấn hiện tại thông qua một kênh khác để đảm bảo đây đúng là một Người phỏng vấn mới đến từ nguồn yêu cầu ban đầu
- Xác nhận thành viên Người phỏng vấn mới đã ký kết biên bản bảo mật thông tin trước khi cấp quyền truy cập vào hệ thống làm việc
- Xác nhận Người phỏng vấn mới đã hoàn thành khóa đào tạo cơ bản về các module CATI
- Kiểm tra Người phỏng vấn mới phải tạo tài khoản trên research.t5r.vn
- Kiểm tra xem Người phỏng vấn mới có quyền quản trị viên trên tài khoản của chính mình trong tab Truy cập hay không
- Kiểm tra mật khẩu đã được thay đổi không muộn hơn 1 tuần sau ngày bắt đầu dự kiến
- Kiểm tra gửi thư thông báo cho người phỏng vấn mới và yêu cầu họ nhớ thay đổi mật khẩu tên người dùng của Người phỏng vấn

Quản trị người dùng/mật khẩu

- Bạn chỉ được phép sử dụng tài khoản đăng nhập cá nhân của mình để truy cập vào bất kỳ hệ thống nào chứa thông tin cá nhân. Tuy nhiên, nếu công việc của bạn liên quan đến quản trị IT, bạn có thể truy cập bằng tài khoản quản trị riêng, nhưng vẫn phải tuân thủ các quy trình dành riêng cho hoạt động quản trị IT.
- Trường hợp bạn biết được mật khẩu đăng nhập của người khác, bạn cần ngay lập tức thông báo cho người đó về vấn đề này và đảm bảo rằng bạn không còn quyền truy cập vào tài khoản của họ sau đó. Tương tự, nếu ai đó biết được mật khẩu đăng nhập của bạn, bạn phải đổi mật khẩu ngay lập tức.
- Nếu hệ thống chứa dữ liệu cá nhân hỗ trợ xác thực hai lớp (2FA), bạn phải kích hoạt tính năng này. Bạn nên thay đổi mật khẩu thường xuyên.

Khóa thiết bị và bàn làm việc sạch sẽ

- Bất kỳ thiết bị nào, bao gồm máy tính, điện thoại, máy tính bảng, v.v., được sử dụng để truy cập thông tin cá nhân của công ty phải được khóa và màn hình không được hiển thị bất kỳ thông tin cá nhân nào khi không sử dụng.
- Tất cả thông tin cá nhân, bất kể được lưu trữ trên giấy tờ, thiết bị lưu trữ di động, hay ổ cứng gắn trong thiết bị, đều phải được bảo mật an toàn hoặc tiêu hủy đúng cách khi không sử dụng
- Tất cả giấy tờ chứa thông tin cá nhân phải được xử lý theo cách làm cho thông tin đó không thể đọc được.
- Không được để chìa khóa ngăn kéo, tủ, v.v. nếu không có sự giám sát.
- Máy in và máy fax cũng cần được tuân theo các chính sách tương tự như trên:
  - Bất kỳ lệnh in nào chứa thông tin cá nhân đều phải được thực hiện ngay lập tức
  - Mọi giấy tờ phải được hủy bỏ hoặc xử lý vào cuối ngày làm việc.

Thông tin cá nhân trong bảng điều khiển

Trong trường hợp này, T5Research là Bên kiểm soát dữ liệu, do đó quyền truy cập vào thông tin cá nhân được kiểm soát bởi các quy trình nội bộ của chúng tôi.

- Bất kỳ DCS nào trên bảng điều khiển đều phải được mã hóa tên.
- Bất kỳ hình thức báo cáo nào trên bảng điều khiển dữ liệu phải được ẩn danh hoàn toàn.
- Bất kỳ dữ liệu bảng điều khiển nào được xuất ra khỏi văn phòng đều phải được ẩn danh hoàn toàn.

Dữ liệu cá nhân từ khách hàng

Trong bối cảnh này, T5Research là đơn vị xử lý dữ liệu, do đó mọi quyền truy cập vào dữ liệu khách hàng đều bị hạn chế, cả quy trình nội bộ của chúng tôi cũng như bất kỳ quy trình cụ thể nào mà chúng tôi có thể đã thỏa thuận với khách hàng.
Do đó, tất cả các yêu cầu được đề cập ở trên đều có hiệu lực, cùng với bất kỳ yêu cầu nào từ khách hàng. Cụ thể, thường sẽ có các yêu cầu cụ thể đối với việc trao đổi dữ liệu, ai có thể truy cập dữ liệu và thời gian xóa dữ liệu khỏi hệ thống của chúng tôi.
Ngoài ra, việc thông báo cho Giám đốc Công nghệ (CTO) của khách hàng về bất kỳ rò rỉ hoặc sử dụng sai dữ liệu cá nhân cũng là một yêu cầu bắt buộc, càng sớm càng tốt và chậm nhất là 72 giờ sau khi phát hiện sự cố.

Dữ liệu cá nhân trên nền tảng của T5Research

Trong bối cảnh này, T5Research là đơn vị xử lý dữ liệu và do đó các yêu cầu cũng giống như bên trên.

Các hệ thống khác lưu trữ dữ liệu cá nhân

Quy định GDPR (Quy định về bảo vệ dữ liệu chung) không chỉ áp dụng cho dữ liệu bên trong doanh nghiệp mà còn bao gồm tất cả các hệ thống khác liên quan đến dữ liệu cá nhân. Điều này bao gồm bản tin, đơn xin việc, quản lý lương, thông tin đăng nhập trang chủ và nhiều nơi khác. Bên cạnh đó, bất kỳ hệ thống riêng lẻ nào xử lý dữ liệu cá nhân đều phải có chính sách GDPR riêng hoặc được bao phủ bởi chính sách GDPR khác.
Do đó, bất kỳ hệ thống mới nào xử lý dữ liệu cá nhân đều phải được CTO (Giám đốc Công nghệ) phê duyệt. Nếu bạn phát hiện dữ liệu cá nhân ở bất kỳ đâu nhưng lại thiếu chính sách GDPR hoặc chính sách hiện tại chưa đầy đủ, vui lòng liên hệ với CTO.

Yêu cầu pháp luật

GDPR quy định một danh sách các quyền của mỗi cá nhân, đồng thời đưa ra các yêu cầu về lưu trữ dữ liệu cá nhân.

Quyền minh bạch và sử dụng

Theo quy định của GDPR, bất kỳ thông tin và liên lạc nào liên quan đến việc xử lý dữ liệu cá nhân phải dễ dàng truy cập và dễ hiểu, đồng thời phải sử dụng ngôn ngữ rõ ràng và đơn giản. Ngoài ra, cần phải nêu rõ dữ liệu cá nhân được sử dụng để làm gì và ai có quyền truy cập vào dữ liệu đó.

Quyền truy cập nguồn dữ liệu

Nếu một người không được yêu cầu trực tiếp cung cấp thông tin cá nhân của họ, thì người đó có quyền được biết nguồn gốc của dữ liệu. Ví dụ: Nếu có một cuộc khảo sát mà chúng tôi nhận được danh sách người trả lời từ khách hàng, nhưng một phần trong yêu cầu của dự án là phải giấu nguồn với người trả lời, thì người trả lời đó vẫn có quyền được biết. Tuy nhiên, không có gì ngăn cản chúng tôi không hoàn thành phỏng vấn với người trả lời được cung cấp.

Quyền được lãng quên

Một trong những yêu cầu pháp lý quan trọng nhất là quyền được lãng quên trong bất kỳ hệ thống nào chứa thông tin cá nhân. Đối với chúng tôi, có 2 tình huống liên quan đến việc xóa thông tin cá nhân của một người.

1. Sau khi việc sử dụng thông tin cá nhân hoàn tất, thì thông tin cá nhân đó phải được xóa bỏ.

Điều này có liên quan đến một vài trường hợp khác nhau:

a) Khi bạn thu thập dữ liệu cá nhân của người tham gia khảo sát, bạn có trách nhiệm bảo vệ thông tin đó. Điều này bao gồm việc xóa bỏ thông tin cá nhân khi không còn cần thiết nữa. Luật pháp không quy định cụ thể thời điểm phải xóa thông tin cá nhân. Tuy nhiên, bạn cần xác định rõ ràng thời điểm xóa trong quy trình thu thập và sử dụng dữ liệu.

b) Sau một khoảng thời gian “dài” nếu người dùng không còn muốn sử dụng hệ thống nữa, thì thông tin nhận dạng cá nhân của người đó phải bị xóa bỏ. Một lần nữa, luật pháp không quy định thời gian cụ thể, mà chỉ yêu cầu mọi hoạt động lưu trữ thông tin cá nhân phải đi kèm với chính sách xóa dữ liệu.

2. Một cá nhân có thể yêu cầu chúng tôi xóa thông tin của họ, đây còn được gọi là "quyền được lãng quên". Nếu chúng tôi chỉ là đơn vị xử lý dữ liệu (data processor), thì yêu cầu này cũng có thể đến từ bên kiểm soát dữ liệu (data controller).

Quyền tải dữ liệu

Một người có quyền yêu cầu nhận toàn bộ thông tin cá nhân của mình. Lưu ý rằng việc xác minh danh tính của người yêu cầu trước khi cung cấp thông tin là rất quan trọng để ngăn chặn rò rỉ dữ liệu.

Quyền sửa thông tin không chính xác

Mọi người có quyền yêu cầu sửa thông tin cá nhân của họ nếu thông tin đó không chính xác hoặc không đầy đủ.

Quyền khiếu nại

Cá nhân có quyền khiếu nại với cơ quan giám sát