Tiêu chuẩn Toàn cầu: Phân biệt giữa Bên kiểm soát và Bên xử lý trong Pháp luật về Bảo mật dữ liệu

Một hệ thống pháp luật toàn diện về bảo mật dữ liệu phải đặt ra những nghĩa vụ chặt chẽ cho tất cả các công ty quản lý dữ liệu của người tiêu dùng. Tuy nhiên, những nghĩa vụ ấy sẽ chỉ đủ mạnh để bảo vệ quyền riêng tư và củng cố niềm tin của người tiêu dùng nếu chúng phản ánh được cách mà một công ty tương tác với dữ liệu của người tiêu dùng.

Pháp luật về bảo mật dữ liệu trên thế giới thường phân biệt hai loại công ty: (1) những doanh nghiệp quyết định cách thức và lý do thu thập dữ liệu người tiêu dùng, đóng vai trò là **bên kiểm soát** dữ liệu đó và (2) những doanh nghiệp xử lý dữ liệu thay mặt cho công ty khác, đóng vai trò là **bên xử lý** dữ liệu.

Sự khác biệt cơ bản này có ý nghĩa đặc biệt quan trọng đối với một loạt các đạo luật về bảo mật dữ liệu trên toàn thế giới, bao gồm Quy định bảo vệ dữ liệu chung của Liên minh Châu Âu ("GDPR") và Đạo luật bảo vệ dữ liệu người tiêu dùng của California ("CCPA"). Cả hai loại công ty đều có những trách nhiệm và nghĩa vụ quan trọng, cần được quy định trong bất kỳ hệ thống pháp luật nào.

Ai quản lý dữ liệu của người tiêu dùng?

NGƯỜI TIÊU DÙNG

Các cá nhân sở hữu dữ liệu cá nhân bị bên kiểm soát thu thập và sử dụng

VÍ DỤ

Người tiêu dùng mua sắm tại các cửa hàng bán lẻ, mua hàng qua mạng, hoặc chia sẻ thông tin trên các nền tảng mạng xã hội.

NGƯỜI TIÊU DÙNG CẦN CÓ QUYỀN:

- **Được biết** bên kiểm soát dữ liệu thu thập loại dữ liệu nào — và vì sao
- **Từ chối,** và lựa chọn không tham gia vào các hình thức sử dụng dữ liệu, không chỉ giới hạn ở hình thức mua bán
- **Truy cập** các thông tin về họ
- **Hiệu chỉnh** các thông tin đó
- **Xóa bỏ** các thông tin đó
- **Được đảm bảo an toàn** về dữ liệu của họ
- Được đảm bảo rằng dữ liệu của họ được **sử dụng đúng mục đích**

BÊN KIỂM SOÁT

Quyết định có thu thập dữ liệu từ người sử dụng hay không, cách thức thu thập và mục đích sử dụng dữ liệu

VÍ DỤ

Các công ty tương tác trực tiếp với người tiêu dùng như khách sạn, ngân hàng, cửa hàng bán lẻ, đại lý lữ hành, và nhà cung cấp công nghệ làm việc trực tiếp với khách hàng.

BÊN KIỂM SOÁT CÓ TRÁCH NHIỆM:

Xin sự đồng ý cần thiết để xử lý dữ liệu của người tiêu dùng

Đáp ứng yêu cầu truy cập, hiệu chỉnh hoặc xóa dữ liệu của người tiêu dùng

Sử dụng dữ liệu phù hợp với kỳ vọng của người tiêu dùng

BÊN XỬ LÝ

Xử lý dữ liệu thay mặt cho bên kiểm soát, theo yêu cầu của bên kiểm soát

VÍ DỤ

Các công ty cung cấp các sản phẩm giữa doanh nghiệp với doanh nghiệp như điện toán đám mây, các nhà cung cấp dịch vụ in ấn, chuyển phát, và các công ty xử lý dữ liệu theo yêu cầu của một công ty khác.

BÊN XỬ LÝ CÓ TRÁCH NHIỆM:

Xử lý dữ liệu theo đúng yêu cầu của bên kiểm soát

Áp dụng các biện pháp phòng vệ thích hợp được thiết kế để đảm bảo an toàn dữ liệu

Các bên kiểm soát và bên xử lý cần có trách nhiệm tương ứng với vai trò của mình để đảm bảo tính bảo mật và an toàn thông tin của người tiêu dùng.

Pháp luật về Bảo mật dữ liệu trên thế giới có sự phân biệt giữa Bên kiểm soát và Bên xử lý dữ liệu

Pháp luật về bảo mật dữ liệu trên thế giới đều phản ánh sự khác biệt cơ bản giữa các công ty quyết định thu thập và sử dụng dữ liệu của cá nhân và các công ty chỉ xử lý dữ liệu đó.

Các công ty quyết định cách thức và lý do thu thập dữ liệu người tiêu dùng.	Các công ty xử lý dữ liệu của người tiêu dùng theo yêu cầu của bên thứ ba.
GDPR: Bên kiểm soát Xác định "mục đích và phương thức" xử lý.	**GDPR: Bên xử lý** Xử lý dữ liệu cá nhân "thay mặt cho" bên kiểm soát.
CCPA: Doanh nghiệp Xác định "mục đích và phương thức" xử lý.	**CCPA: Bên cung cấp dịch vụ** Xử lý dữ liệu cá nhân "thay mặt cho" doanh nghiệp.

Sự khác biệt này có ý nghĩa đặc biệt quan trọng đối với một loạt các đạo luật về bảo mật dữ liệu, không chỉ giới hạn ở GDPR và CCPA. Hơn nữa, các tiêu chuẩn bảo mật hàng đầu thế giới, bao gồm ISO 27701 và các khuôn khổ tự nguyện nhằm đảm bảo khả năng chuyển giao dữ liệu xuyên biên giới quốc gia, như Quy tắc trao đổi dữ liệu cá nhân xuyên biên giới APEC, cũng phân biệt giữa bên kiểm soát và bên xử lý dữ liệu.

VÍ DỤ

Một doanh nghiệp giao kết hợp đồng với một công ty in ấn để làm thiệp mời cho một sự kiện. Doanh nghiệp này cung cấp cho công ty in tên và địa chỉ của các khách mời từ cơ sở dữ liệu liên lạc của mình, từ đó công ty in sử dụng để in lên các thiệp mời và phong bì. Doanh nghiệp sau đó gửi các thiệp mời đi.

Doanh nghiệp là bên kiểm soát dữ liệu cá nhân đã được xử lý liên quan đến các thiệp mời. Doanh nghiệp quyết định mục đích mà dữ liệu cá nhân được xử lý (để gửi thiệp mời cho từng cá nhân theo địa chỉ tương ứng) và phương thức xử lý (gửi thư gộp dữ liệu cá nhân bằng cách sử dụng địa chỉ của khách mời). Công ty in là bên xử lý dữ liệu cá nhân theo yêu cầu của doanh nghiệp. Công ty in không được phép bán dữ liệu hoặc sử dụng nó cho những mục đích khác, ví dụ như tiếp thị. Nếu công ty in bỏ qua các hạn chế trên và sử dụng dữ liệu cho mục đích riêng của mình, công ty in sẽ trở thành bên kiểm soát dữ liệu và phải tuân thủ mọi nghĩa vụ được đặt ra cho bên kiểm soát.

Vì sao việc phân biệt Bên kiểm soát và Bên xử lý quan trọng đối với hoạt động bảo vệ dữ liệu của người tiêu dùng?

Việc phân biệt giữa bên kiểm soát và bên xử lý sẽ đảm bảo rằng những nghĩa vụ mà pháp luật quy định về bảo mật dữ liệu phản ánh đúng vai trò của một công ty trong quá trình quản lý dữ liệu của người tiêu dùng. Điều này giúp bảo vệ quyền riêng tư của người tiêu dùng, không vô tình tạo ra những rủi ro mới về bảo mật hoặc an ninh.

Bảo vệ Dữ liệu. Cả bên kiểm soát và bên xử lý đều cần tuân thủ các nghĩa vụ chặt chẽ để bảo vệ dữ liệu của người tiêu dùng.

- Việc đặt ra nghĩa vụ này cho cả hai loại công ty đảm bảo rằng dữ liệu của người tiêu dùng luôn được bảo vệ.
- Bên kiểm soát và bên xử lý cần áp dụng các biện pháp bảo mật hợp lý và phù hợp, tương ứng với dung lượng và mức độ nhạy cảm của dữ liệu, quy mô và bản chất của doanh nghiệp, cũng như chi phí cho các công cụ sẵn có.

Quyền yêu cầu của người tiêu dùng. Để đáp ứng các yêu cầu quan trọng về quyền lợi của người tiêu dùng - chẳng hạn yêu cầu truy cập, hiệu chỉnh và xóa bỏ dữ liệu cá nhân - cần thiết phải biết nội dung của dữ liệu đó là gì.

- Bên kiểm soát tương tác với người tiêu dùng và quyết định thời điểm và lý do thu thập dữ liệu của họ. Vì vậy, các bộ luật như GDPR và CCPA yêu cầu bên kiểm soát phản hồi các yêu cầu về quyền lợi của người tiêu dùng. Ngoài ra, bên kiểm soát phải quyết định liệu có lý do từ chối yêu cầu của người tiêu dùng hay không, chẳng hạn khi người tiêu dùng yêu cầu xóa thông tin thuộc phạm vi lưu trữ hợp pháp.
- Ngược lại, bên xử lý thường không biết nội dung dữ liệu mà họ sẽ xử lý và có thể bị cấm xem các nội dung này theo thỏa thuận hợp đồng. Vì vậy, sẽ không phù hợp nếu để bên xử lý phản hồi trực tiếp các yêu cầu của người tiêu dùng. Điều này có thể tạo ra cả rủi ro về an ninh (cung cấp dữ liệu cho những người tiêu dùng mà họ không biết) lẫn rủi ro về quyền riêng tư (xem các dữ liệu mà họ không được phép xem). Thay vào đó, bên xử lý nên cung cấp cho bên kiểm soát các công cụ mà bên kiểm soát có thể sử dụng nhằm thu thập dữ liệu cần thiết để đáp ứng yêu cầu của người tiêu dùng.