INFOSUM

How to preserve consumer trust while collaborating

First-party data collaboration is vital to enable marketers to deliver high performing marketing in the post-cookie world. At the same time, you need consumers to trust that you'll responsibly handle any personal information they choose to give you.

Use this checklist to enable privacy-safe data collaboration.

Do you have permission from customers to collaborate?

Ensure valid legal basis for collecting data for marketing purposes

The goal when collecting personal data is to clearly communicate the value exchange in order to gain consent that allows you to use their data for marketing purposes.

Prevent the daisy-chaining of consent. Daisy-chaining occurs when consent, and therefore permission to use that data, is passed from one party to another without a user being fully aware.

An example of this is in programmatic where there are often multiple ad tech platforms syncing data in the form of cookies. Once in effect, it becomes incredibly difficult to protect consumer data due to the sheer amount of intermediaries involved.

How will you retain control of your data?

Ensure your data is not centralised and commingled with another party's data

Avoid solutions that require you to transfer data to a third-party where it is pooled and commingled with other company's data. This results in you losing control of your data and adds more complexity around data privacy and security reviews.

We recommend choosing a decentralised solution that by design avoids the need to pool or commingle data, enabling you to maintain consumer trust while dramatically reducing the compliance drag.

Ensure your data isn't locked into a third-party ID data silo

Third-party IDs are being deprecated by changes to browser technology, driven by concerns over the lack of privacy control they offer consumers. To ensure you are both protecting consumer privacy and future-proofing your marketing, these should be avoided.

Enable privacy-safe data collaboration by choosing a federated and decentralised solution that only works on first-party data to deliver high performing, people-based marketing.

How will you be protecting your customers identity?

When collaborating across multiple data sets, ensure insights are anonymised

In order to unlock marketing insights through collaboration, data sets containing personal data often need to be brought together for analysis. To prevent individuals from being identified during analysis, data is either pseudonymised or anonymised:

Pseudonymisation:
Personal data can no longer be attributed to an individual without additional information.

Anonymisation:
Personal data can no longer be attributed to an individual.

Which should you choose?

Be aware of regional privacy laws and legislation: Under the GDPR, for example, pseudonymised data is still classified as personal data.

When conducting analysis across multiple data sets, choose a solution that generates anonymous, statistical results that can be safely used to drive marketing insights while protecting customer identity.

Ensure your chosen solution uses differential privacy techniques

Differential privacy is a method of enabling sensitive personal data to be analysed while ensuring no information is ever exposed that can be used to identify an individual.

When collaborating across multiple data sources, make certain differential privacy techniques are being applied, to ensure your customers can never be re-identified during analysis.

Ability to rescind another party's access to your data when a relationship ends

When collaborating across multiple parties and data sets, how do you retain control of your data and prevent access once a commercial relationship has ended?

Decentralised marketing infrastructure solutions, such as InfoSum, provide you with far greater control over your customer data. The non-movement of data, combined with rich permission systems means you can easily control who can analyse your data and for how long.

For more information, visit: www.infosum.com