Top 5 Questions to Ask of your Data Supplier to Ensure GDPR Compliance, Avoid Millions in Fines

Rhetorik

Top 5 Questions to Ask of your Data Supplier
to Ensure GDPR Compliance, Avoid Millions in Fines

Is your B2B contact data affected by GDPR? How deep do you need to track compliance in your data vendors? Are you a controller or a processor? How much of your worldwide revenue is at risk? Read on to get more context and learn the 5 most important questions to ask your Data Supplier.

GDPR in a Nutshell

The GDPR is the strongest global privacy law in effect today, and was created to regulate how organizations collect, handle, and protect personal data of EU residents. GDPR was designed to strengthen privacy rights by giving data subjects (defined as any person formally residing in the EU who has their data collected, held, or processed by a controller or processor) control of how their personal data is obtained, used and shared.

Cookies, Privacy Notices, Data Breaches and More

What do Google, British Airways, H&M and Marriott all have in common? They all received fines in excess of €10,000,000 for GDPR violations relating to personal data, and affecting upwards of 383 million customer records.

Even more staggering, Amazon's gigantic €746 million GDPR fine, announced in the company's July 2021 earnings report, nearly 15 times bigger than the previous record.

What Went Wrong?

- In the case of Amazon, the largest fine to date, it attempted to force users to "agree" to cookies—or make opting out of cookies difficult—to collect as much personal data as possible. Lesson learned? Obtain "freely given", informed, and unambiguous opt-in consent before setting cookies on users' devices.
- WhatsApp's somewhat opaque privacy notice was their downfall. The company should have provided privacy information in an easily accessible format using language its users could quickly understand.
- Google's cookie policy was fundamentally flawed. Under the GDPR, consent must be "freely given" – equally easy to accept or refuse. If you can accept with one click, you should also be able to refuse with one click.
- H & M violated the GDPR's principle of data minimization — don't process personal information, particularly sensitive data about people's health and beliefs, unless you need to for a specific purpose. H&M should have placed strict access controls on the data, and the company should not have used this data to make decisions about people's employment.
- In the case of British Airways and Marriott, breaches were preventable. Neither company had sufficient security measures in place to protect their systems, networks, and data. In fact, British Airways lacked the basics, such as multi-factor authentication, at the time of the breach. Taking a security-first approach, investing in security solutions, and ensuring strict data privacy policies and procedures are in place are fundamental to GDPR compliance.

What's My Role?

Generally speaking, there are two types of parties that have a responsibility regarding the handling of data: the "controller" and the "processor." It is important to determine whether you are acting as a controller or a processor and understand your responsibilities accordingly.

Data Controller

A data controller determines the purposes, conditions, and means of the use of personal data.

Data Processor

A data processor on the other hand only acts on the instructions of the "controller" and processes personal data on their behalf.

Any reseller of data becomes the controller in relation to the customer's data.

Here's the thing: You can't be GDPR compliant if you don't start GDPR compliant.

It goes without saying that the core of a successful marketing strategy is strong data. What do we mean by strong? Clean, accurate, comprehensive, and, most importantly, compliant.

What is critical is understanding the nuances of first-party and third-party data to leverage each in a way that allows you to serve relevant messages and content to your target audiences. As privacy laws crack down on third-party data, it will soon become more difficult for marketers to deliver on their goals.

First party data refers to the data collected through your own marketing campaigns when people voluntarily give you their information in exchange for your offer.

For example, someone wants to take advantage of a free trial or demo you're promoting in exchange for completing a form with their information, including name, job title, company, and contact information. In this case, the prospect has voluntarily opted-in to receive communications from your organization.

In contrast, third party data is collected from sources other than your own. Unlike first-party, it's not restricted to only those who have already shown interest in your company. The primary advantage of using third-party data is that it expands your universe of prospects providing incremental target customers who may not have heard of your solutions, or may even be interested in your competitors. There are restrictions that come with using third-party data, particularly around privacy. GDPR regulation requires a controller to comply with one of six legal bases to acquire and process a prospect's data.

Before acquiring a contact list or a database with contact details of individuals from another organization, that organization must be able to demonstrate that the data was obtained in compliance with the GDPR, and that it may use it for marketing purposes. If the organization processes the data based on legitimate interest, the data subject must have been notified (see 'Right to be Informed' below) about that processing, its purpose and informed of their rights. So what does that all mean? It's crystal clear.

Without the legal bases to acquire and process a prospect's data, a company acquiring third-party data cannot be GDPR compliant, no matter what additional efforts they undertake.

Want to learn more, schedule a demo or take advantage of our free trial?

Visit Us Online

www.rhetorik.com

Trusting your Data Provider: Top 5 Questions to ask of your Data Supplier to ensure GDPR Compliance

Generally speaking, there are two types of parties that have a responsibility regarding the handling of data: the "controller" and the "processor." It is important to determine whether you are acting as a controller or a processor and understand your responsibilities accordingly.

1. Does the vendor have the right processes in place?
2. How will / does the vendor help to respond to Data Subject rights requests?
3. Does the vendor provide privacy impact assessments?
4. Is the vendor implementing the GDPR 'security principle', by applying 'appropriate technical and organisational measures'?
5. Does the vendor know all the types of customer data they are collecting, and how long are they storing it for?

At Retorik, privacy and compliance are number one. Our data is clean, accurate, standardized, and continuously maintained. Most importantly, we human-verify our data to ensure GDPR compliance from the source, reducing your risk of non-compliance and resulting fines.

Personal Data and GDPR

Under GDPR, personal data is any data that is linked to the identity of a living person. This includes not only direct associations, such as financial information and addresses, but also indirect links, such as evaluations relating to the behavior patterns of a person. The definition of personal data is also format-agnostic, so it could include images, video, audio, numerals, and words. Inaccurate information relating to data subjects is still considered personal data because this information is linked to an identity.

On its website, the European Commission defines personal data as:

- A name and surname
- A home address
- An email address
  ex: name.surname@company.com
- An identification card number
- Location data
  ex: the location data function on a mobile
- An Internet Protocol (IP) address
- A cookie ID
- The advertising identifier of your phone
- Data held by a hospital or doctor, which could be a symbol that uniquely identifies a person

As importantly, it also lists examples of what is not considered personal data. These examples are:

- A company registration number
- An email address such as info@company.com
  ex: info@company.com
- Anonymized data

The GDPR also makes a clear distinction between personal data and sensitive data via the "Special Categories". The Special Category includes:

- Race and ethnic origin
- Religious or philosophical beliefs
- Trade union memberships
- An identification card number
- Biometric data used to identify an individual
- Genetic data
- Health data
- Data related to sexual preferences, sex life, and/or sexual orientation

The processing of special category data is prohibited unless:

- "Explicit consent" has been obtained from the data subject, or,
- Processing is necessary in order to carry out obligations and exercise specific rights of the data controller for reasons related to employment, social security, and social protection, or,
- Processing is necessary to protect the vital interests of data subjects where individuals are physically or legally incapable of giving consent, or,
- Processing is necessary for the establishment, exercise, or defense of legal claims, for reasons of substantial public interest, or reasons of public interest in the area of public health, or,
- For purposes of preventive or occupational medicine, or,
- Processing is necessary for archiving purposes in the public interest, scientific, historical research, or statistical purposes, or,
- Processing relates to personal data which are manifestly made public by the data subject, or,
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subject.

Compliancy

Fundamentally, GDPR Compliance means an organization that falls within the scope of the GDPR meets the requirements for properly handling personal data as defined in the law.

The GDPR outlines certain obligations organizations must follow which limit how personal data can be used. It also defines nine data subject rights, plus the right to withdraw consent. Organizations have one month's time to respond to a data subject inquiring about their rights.

1. RIGHT TO BE INFORMED

   Data subjects have the right to be informed about the collection and use of their personal data.

2. RIGHT TO ACCESS

   Data subjects have the right to view and request copies of their personal data.

3. RIGHT TO RECTIFICATION

   Data subjects have the right to view and request copies of their personal data.

4. RIGHT TO RECTIFICATION

   Data subjects have the right to request inaccurate or outdated personal information be updated or corrected.

5. RIGHT TO BE FORGOTTEN / RIGH TO ERASURE

   Data subjects have the right to request their personal data be deleted.

6. RIGHT FOR DATA PORTABILITY

   Data subjects have the right to ask for their data to be transferred to another controller or provided to them. The data must be provided in a machine-readable electronic format.

6. RIGHT TO RESTRICT PROCESSING

   Data subjects have the right to request the restriction or suppression of their personal data.

7. RIGHT TO OBJECT

   Data subjects have the right to request the restriction or suppression of their personal data.

8. RIGHT TO OBJECT TO AUTOMATED PROCESSING

   Data subjects have the right to object to decisions being made with their data solely based on automated decision making or profiling.

9. RIGHT TO WITHDRAWL CONSENT

   Data subjects have the right to withdraw previously given consent to process their personal data.

Rhetorik

Rhetorik provides enterprise grade solutions for all users of global profile data.
Get started at rhetorik.com or +44 (0)118 989 8580