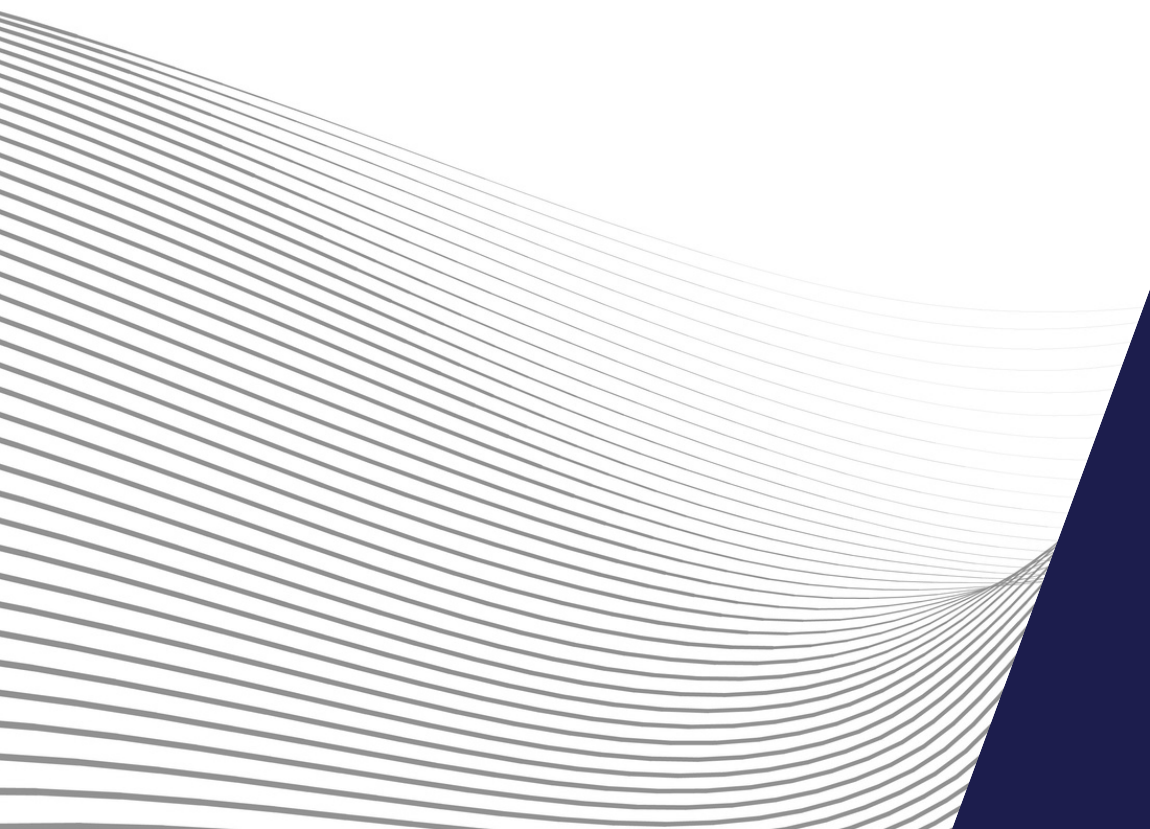
QUADRANT

CONSENT MANAGEMENT

ANSWERING THE WHAT, WHY, AND HOW



EBOOK

OVERVIEW

In today's intricate digital economy, customers have more choices than ever. To remain profitable, businesses need to reduce customer churn, retain existing clients, and improve their lifetime value. But why do customers turn away from a business?

Today's users are driven by experience - ease of use, innovation, speed, consistency, and the most important of all, trust. To deliver personalised experiences, many businesses leverage data collected on digital platforms like websites and mobile applications. While this data can fuel growth, users will get frustrated and question your business integrity if there are no constraints on using their data.

Acknowledging your users, respecting their privacy, and seeking their permission can create exceptional business value with minimal user frustration. However, most business owners are unsure of how to address privacy and consent.

The current regulatory environment further complicates things. The law expects companies to be compliant, which takes resources away from their primary business activities.

In this e-book, we demystify "user consent" and show you how to build a user-centric system that helps you stay compliant and win customer trust.

DATA MISUSE AND THE NEED FOR USER CONSENT

Used in the right manner, data can potentially cure cancer, close the wage gap, and prevent us from catching an infectious disease (like Covid-19). But the misuse of personal data is all too common. We have seen many examples in the last few years where businesses and governments violated the spirit - and often the letter - of privacy laws.

The data breach at Equifax, the Facebook–Cambridge Analytica data scandal, reports about audio data collected by smart speakers like Amazon Echo, privacy concerns around DNA data collected by 23andMe, and countless other incidents have escalated people's concerns around the misuse of their personal information.

As a result, regulatory bodies worldwide have introduced strict compliance mandates to control how businesses collect and manage data. As a general rule, data collectors should obtain explicit consent from consumers before using their personal information, and failure to comply can lead to monetary fines, reputational damage, and lawsuits.

Source: The Guardian on YouTube

Over 100 countries enacted data privacy laws, of which at least 41 mention user consent specifically. Some of the regulations that have stringent conditions for gathering user consent are:

EU's General Data Protection Regulation (GDPR)

California Consumer Privacy Act (CCPA)

Brazilian General Data Protection Law (LGPD)

Australia's Privacy Principles/Privacy Act (APP)

Singapore's Personal Data Protection Act (PDPA)

Did you know - Consent violations under GDPR are classified under 'Insufficient legal basis for data processing.' So far, 156 fines (the highest number) amounting up to €128,919,040 (approx) have been levied under this category.

Source: www.enforcementtracker.com

WHAT IS USER CONSENT?

“User consent” has varying definitions in different jurisdictions. Broadly speaking, user consent is the agreement for storing, using, and transferring an individual's data by businesses, researchers, healthcare providers, and more.

For a long time, data acquisition on digital platforms was mostly unregulated. Simply visiting or browsing websites or using mobile applications was considered as implied consent for data processing and usage.

However, the increase in the collection of people's private information for business gains brought along concerns around data rights and privacy. Under various data privacy regulations, the processing of user data requires explicit informed consent.

Apart from being a regulatory requirement, explicit user consent has now become the baseline for the ethical use of data to deliver personalised offerings, create meaningful conversations, or simply improve customer experience.

WHY IS USER CONSENT SO IMPORTANT?

The data collected on digital platforms can provide powerful insights, helping businesses make better, profitable decisions. But with the increased awareness and concerns around data privacy, you now need permission to use your user's data.

Establishing a framework for ethical use is critical, especially when it comes to personally identifiable information. Data privacy laws like the GDPR, CCPA, and others have highlighted this need for privacy and how user data should not be considered a free-for-all resource. These regulations put users in control of their information, and there are strict penalties for processing their data without valid consent. Moreover, user-consent is the new currency of trust. To earn consumers' trust and business, companies need to exhibit their seriousness towards data integrity.

HOW TO MANAGE USER CONSENT

We have established the need for ethical data use and introduced the concept of consent. In practical terms, you need to build a new a whole new process of gathering user consent and handling its entire lifecycle within your digital platforms.

This process is called Consent Management. It helps your business gather consent from customers to use, store, manage, and share their data while allowing them to modify or opt-out of their earlier preferences at any time.

THE PROCESS OF CONSENT MANAGEMENT

1. Inform users that their data is being collected when they first visit your website or open your mobile application.
2. Provide information about what data points are being collected.
3. Allow your users to decide if they agree to the specific purposes of data processing.
4. Record consent data in an accessible format with a timestamp.
5. Allow users to change previous permissions or to withdraw consent.
6. Provide users with options to request access to, or deletion of their data.

But how do you build these settings and capabilities into your digital products and websites? How do you efficiently record, manage, and lawfully process user data? How do you provide your users with the option to modify or opt-out of earlier agreements and maintain an accurate record of consent-related activities?

CONSENT MANAGEMENT PLATFORMS

A Consent Management Platform (CMP) is an automated solution that manages the entire lifecycle of permissions around the usage of an individual's personal data. A CMP helps you:

1. Manage the entire lifecycle of the choices a user makes with your digital platform.
2. Save time, cost, and effort required to manage consent manually.
3. Build user trust with a transparent data collection process.
4. Improve data quality by gathering genuine interest from users.
5. Maintain a record of all consent activities to respond to internal or regulatory audits when needed.
6. Stay compliant with data privacy laws and avoid monetary losses due to non-compliance penalties.
7. Focus on your core business without having to reallocate costs and resources for compliance.

> *Gartner predicts that in 2023, brands that put in place user-level control of marketing data will reduce customer churn by 40% and increase lifetime value by 25%. Customer churn can be reduced by giving users more control, not less, over their data.*

Source: Gartner Predicts 2019: In Search of Balance in Marketing Report

WHY DO YOU NEED A CONSENT MANAGEMENT PLATFORM?

YOU ARE IN THE DATA MONETISATION BUSINESS

Many businesses today use data to derive insights that help them grow. Some companies acquire this data from external sources, while some generate their own (for example, mobile application publishers).

Data monetisation is the process of identifying value and creating revenue from your existing data assets. Businesses can also monetise their data by exchanging or selling it or use it to boost advertisement efforts to resell/upsell to their own customers, amongst other things.

With increasing awareness around data privacy and rights, data collectors have a great responsibility at their hands. Businesses now need to introduce greater transparency into consumer data collection to use this data ethically. According to Gartner's Top 10 Trends in Data and Analytics for 2020, by 2022, 35% of large organisations will be either sellers or buyers of data via formal online data marketplaces, up from 25% in 2020. To monetise data assets through data marketplaces, data and analytics leaders should establish a fair and transparent methodology by defining strict data governance and compliance policies.

The global data monetisation market was valued at $44,869 million in 2016, and is projected to reach at $370,969 million by 2023, growing at a CAGR of 35.4% from 2017 to 2023.

Source: 2019 Data Monetisation Market Research Report by www.alliedmarketresearch.com

THE REGULATORY LANDSCAPE IS VERY CONSENT FOCUSED

Privacy regulations have changed how businesses acquire and use user data. Unlike before, your app's continued usage or browsing your website is not considered a valid expression of consent. Data privacy laws such as the GDPR and the CCPA require that:

- Businesses gather explicit consent and maintain proof-of-consent.
- Users are presented with the choice to allow, restrict, or deny the collection of their data.
- Users are able to modify or opt-out of previous consent agreements.
- Businesses delete all data related to a user at the user's request.

Businesses should conduct periodic privacy assessments, upgrade consent procedures with changing guidelines, and document each step of the consent lifecycle to respond to audits when required. Failure to comply with consent conditions and audit deadlines can incur monetary penalties and legal consequences.

Did you know - The French National Commission on Informatics and Liberty (CNIL), fined Google for €50 million. This is the biggest GDPR fine to this date, issued for the lack of transparency on how the data was harvested from data subjects and used for ad targeting. CNIL states that Google failed to provide enough information to users about consent policies.

Source: www,cnil.fr/en

CONSENT CONDITIONS WITHIN VARIOUS REGULATORY LAWS

General Data Protection Regulation (GDPR) – Under GDPR, companies can be fined up to €20 million or 4% of the worldwide annual revenue of the prior financial year, whichever is higher. These fines apply to the infringement of the basic principles for processing personally identifiable information, including conditions for consent, under Articles 4, 6, 7, and 8, 9, and 13, etc.

California Consumer Privacy Act (CCPA) – The CCPA requires businesses to specifically inform consumers about what data is being collected and for what reason. Companies must also give consumers explicit notice and an opportunity to opt-out before re-selling personal information. The CCPA also prohibits selling personal information of a consumer under 16 without consent. Under CCPA, businesses can face a penalty of $2,500 per violation, or up to $7,500 per violation if intentional.

Australia Privacy Act – Based on the Australian Privacy Principals, the deliberate or accidental misuse of personal information, without the individual's consent can lead to fines up to AU$2.1 million for serious or repeated breaches. The penalties can be levied up to AU$10 million, or three times the value of any benefit obtained through the misuse of information, or 10% of a company's annual domestic turnover.

Singapore's Personal Data Protection Act (PDPA) – The PDPA requires organisations to obtain the consent of the individual before collecting, using, or disclosing their personal data and the purpose for which the personal data is collected. Individuals must also be allowed to withdraw consent at any time. The violation of consent terms under PDPA can allow the Personal Data Privacy Commission to levy a financial penalty of up to S$1 million.

DOING IT YOURSELF CAN BE CHALLENGING

Managing user consent for a large volume of users cannot be done manually and must be automated. Data businesses must have deep legal expertise and technical know-how to develop a consent management system that integrate well with their digital platforms. Like with any technology solution, there are two options to implement a CMP: build or buy.

If you are a small-medium business or an independent app developer, you might not have the in-house expertise to build your own consent management platform. Even if you manage to develop one, the cost, effort, and time required to keep it up to date can be taxing. Moreover, the diversity in data privacy regulations requires legal expertise, and your obligations don't end once consent is obtained. You must keep up with changes in regulatory guidelines and new laws as they are introduced.

It is faster, easier, and more cost-effective to use a plug-and-play solution. A configurable third party CMP can be a self-sufficient tool that offers your users complete choice and control over their data while ensuring compliance and minimising your business liability.

CONSENT MANAGEMENT BEST PRACTICES

Given the high stakes compliance environment and the need for a user-centric approach, consent management should be at the core of your data operations. Here are some best practices to establish an effective consent management system:

1. Assess privacy regulations applicable to your country, region, or industry and the terms and conditions for user consent.
2. Build a transparent framework to let users permit or prevent the collection of their data and modify consent parameters with ease.
3. Maintain a record of when consent was obtained, altered, or withdrawn and ensure the utmost security and integrity of these records.
4. Keep consent collection requests separate from generic terms and conditions and avoid technical and legal jargon.
5. Design a simple and uncluttered interface to avoid user frustration keeping smaller form factors and devices in mind.
6. Assess the costs, expertise, and effort required to build an in-house CMP and plan for periodic updates and upgrades.
7. Evaluate a plug-and-play solution based on in-house legal and technical expertise, cost, and ease of integration.

CONCLUSION

Unrestrained use of personal information is no longer a viable way of monetising your digital platforms. Visitation, continued browsing, and accepting cookies are no longer a form of agreement for harvesting user data. Businesses do not have the luxury to ignore the importance of consent collection.

Implementing a consent management platform fosters a user-centric data culture and helps establish compliance with privacy laws, avoiding unwelcome attention from regulators. This culture can give you an ethical and fair usage edge, earning you the trust of customers and resulting in business growth.

QUADRANT'S CONSENT MANAGEMENT PLATFORM FOR MOBILE

The Quadrant Consent Management Platform (QCMP) is a fully featured CMP tailored to mobile application publishers and developers. It covers the whole user consent lifecycle. QCMP is certified by the IAB's Transparency and Consent Framework V2.0 and ensures fair collection and usage of consumer data.

In QCMP, each consent interaction is recorded on an immutable blockchain, ensuring that you are always audit-ready. The best part: QCMP can be added with only a few lines of code into any Android or iOS application, saving time, costs, and effort.

QCMP is currently in closed beta and will be available in early January. To get early access to QCMP, reach out to us at info@quadrant.io. To learn more about QCMP visit our website.

REACH US AT:

www.quadrant.io
info@quadrant.io