A blueprint for robust consent management

Data governance knowledge series – Topic 5

December 2019

pwc

Consent: Overview and requirements

Consent lies at the heart of almost all the data protection and privacy regulations enforced globally. Consent means providing individuals the ability to control and manage usage of their personal information by a data fiduciary or processor. Genuine consent puts individuals in charge of their data. It also helps build trust in the organisation storing and processing personal information. Analysis of some of the global data privacy laws reveals that they have the same underlying consent requirements. Some of the key consent requirements are listed below:

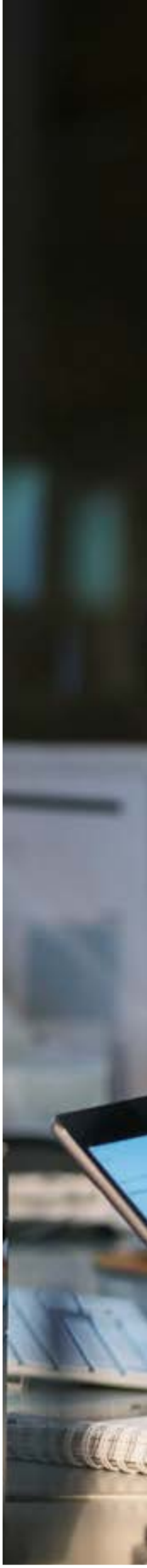
- **Freely given:** It must be truly optional for the data subject.
- **Granular and separate:** Separate consent should be obtained for separate things – separate from terms and conditions and specific to the purpose and methods of the organisation.
- **Unambiguous and clear affirmative action:** It must be clear that individuals intended to provide consent – a clear affirmative action means a clear action to opt-in.
- **Don't use implicit opt-in option:** Avoid using pre-ticked boxes or relying on any other form of silence, inactivity or consent as the default to obtain implicit opt-in.
- **Right to revoke or withdraw consent:** The individual must be informed that he/she can revoke or withdraw his/her consent in a very easy way without any detrimental effect on any of the service currently provided by data processor.

Though organisations are bound to obtain consent from individuals whenever they deal with any kind of personal data in any form or shape, in some exceptional scenarios, consent might not be required – for example, legitimate interest as a basis for processing (e.g. when a bank defaulter's address is shared with a third-party debt collector, or when processing is necessary – e.g. medical history of a patient needs to be disclosed for emergency treatment) or legal obligation (e.g. when processing a particular type of data is a legal obligation, such as the processing of criminal records).

Need for consent management architecture

Consent management architecture has become a critical requirement for enterprises. Today, organisations are focusing on defining full proof consent management processes which can help them in capturing and managing user consent as required by various data protection regulations such as GDPR, CCPA and HIPPA. It is critical that core consent requirements should be considered while defining consent related processes, controls, policies and standards. Once all the basic processes are defined and established, they need to be operationalised and implemented as part of core business processes.

As next steps, organisations should start modelling consent architecture and build a consent management platform which can be used to support consent collection, storage, manage and archival processes. Having a well-defined and robust consent architecture-based platform helps organisations managing all the consent-related requirements given by various regulations. It will reduce manual effort, errors in consent validation process and cost by minimising non-compliance fines.



Components of consent management architecture

Similar to the lifecycle of data (generation, transfer, use, share, storage, archive and destruction), consent management also follows a lifecycle.

Consent is first collected, then stored and processed. Based on the collected and stored consent information ,compliance verification has been performed and only after successful verification data processing gets initiated. Consent can also be modified, which is equivalent to revoking previous consent and giving new consent. Any change in consent, including revocation, needs to be archived for the duration necessary for verification or reconciliation purposes, before it is finally destroyed.

Figure 1: Data and consent lifecycles

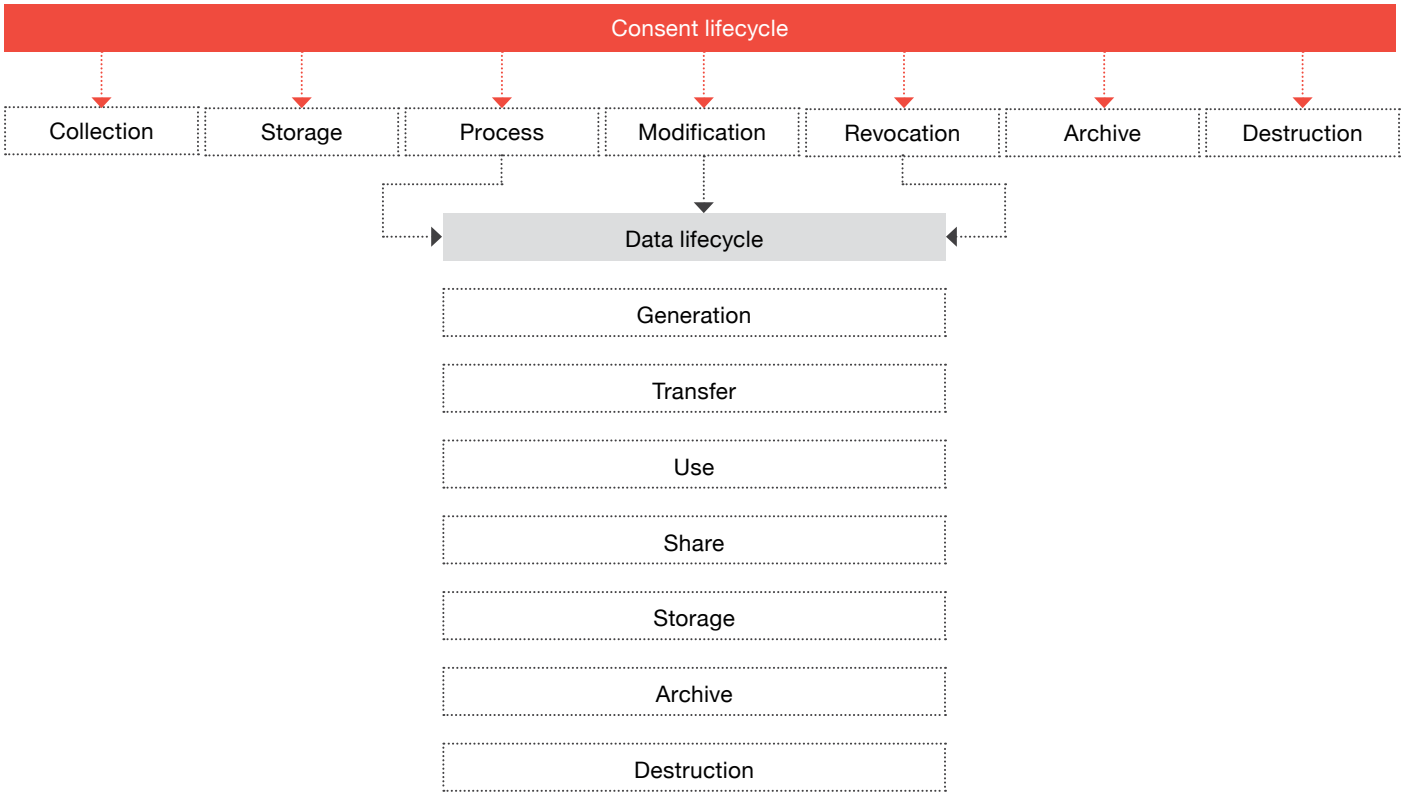
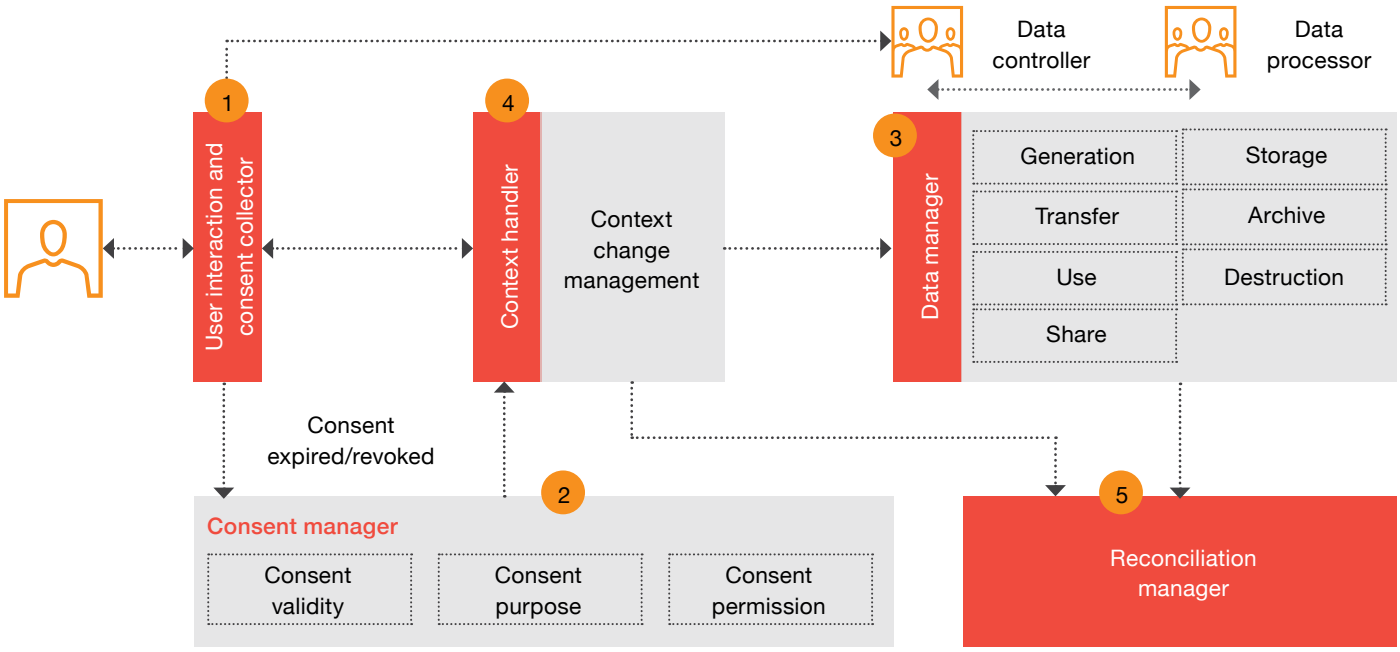


Figure 1 shows the various phases of the consent and data lifecycles. The data lifecycle starts only after the third phase of the consent lifecycle, i.e. the collection of data starts only after the processing of consent, to ensure that the data collection is in compliance with the consent. The consent lifecycle continues even after the end of the data lifecycle, to capture the proof of consent. Any consent management framework or system should adhere to these lifecycles and their relationships.

The above consent lifecycle phases play a critical role in designing the consent platform architecture. The architecture consists of five components (Figure 2).

Figure 2: Consent platform architecture



User interaction and consent collector (CC)

This can be considered as an interface to interact with users and capture consent. It further provides facilities for enforcement of rights, such as data access, erasure and rectification.

Consent manager (CM)

The CM translates the obtained consent into various attributes such as consent validity, consent obligation and consent permission. These attributes can be stored and used for data processing. It enforces the correct behaviour of data handling systems according to the consent and terms of privacy requirements. The consent manager only keeps the up-to-dated consent, which is relevant for the current consent permissions for processing of data. Additional information such as who signed the consent, when the consent was given, and what information was exchanged while providing consent is stored by the reconciliation manager.

Data manager (DM)

The DM ensures adequate permissions for intended usage and processing of data exist, as specified by the consent, before any processing of data, including collection, starts. It is responsible for managing data according to the consent and provides protective control by ensuring only authorised processing of data.

Context handler (CH)

The CH generates a context for a new consent and informs data manager about it. Consent is given for a specific circumstance, e.g. filling online form while signing up for receiving marketing material, doing a transaction/placing an order or subscription to a newsletter. If the purpose of processing the collected data gets changed over time for any reason, e.g. when storage of data might shift to a different cloud storage provider, or he purpose of data collection or usage changes. The CH is responsible for managing context and for detecting those changes of context and informing the consent manager and data manager of these changes. The CM then identifies the change and updates the processing related information, which was created during consent collection. The DM then halts the current processing and checks the new updated permissions for further processing of data.

Reconciliation manager (RM)

The RM is responsible for maintaining and reconciling a processing log of all activities involving data and consent. It records how consent was obtained based on the mechanism used by the user interaction handler to interact with the user, the consent itself from the consent manager, and the activities using the consent. It also keeps a track of the data lifecycle as provisioned by the DM, including activities such as storage and sharing. A record of archived consent and data is also maintained by the RM in events of any context changes and consent revocation. It supports demonstration of the correct behaviour that has been undertaken for compliance reporting purposes.

Consent mechanism

The mechanism of consent differs as per offline and online mode of consent collection. Mainly consent can be obtained in two ways; implicit opt-in and explicit opt-in. Implicit opt-in also known as deemed or indirect consent is usually inferred from data subject's actions and the current circumstance, he/she is in. Explicit opt-in, also known as express or direct consent, means that an individual is clearly presented with an option to agree or disagree with the collection, use, or disclosure of personal information. Some consent is taken over the phone, chat and offline events, and involves third-party vendors. Different regulation policies allow different types of consent for example GDPR does not allow implicit opt-in type of consent.

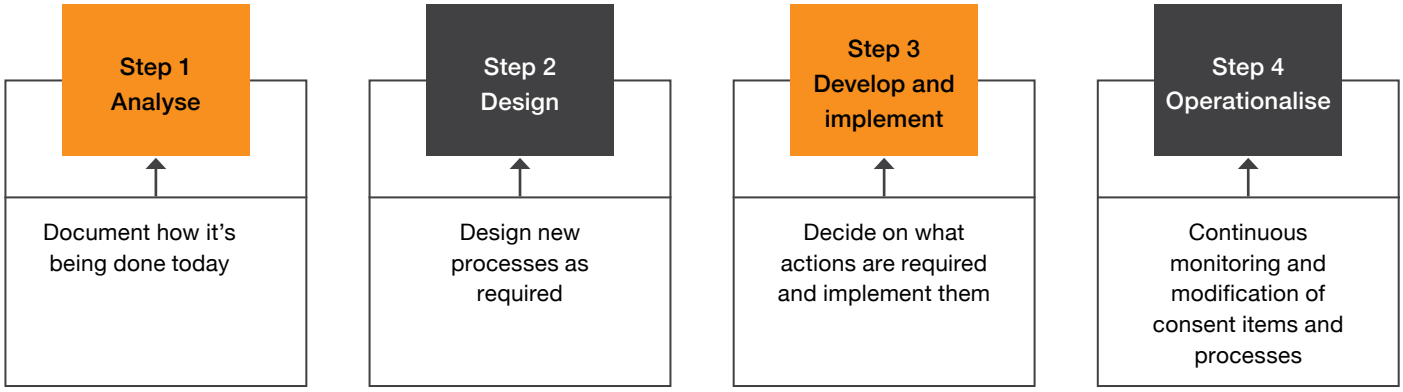
Organisations should adopt consent mechanisms based on their purpose to collect consent, legitimate interests and mode of collection. For example, when consent is obtained via electronic means like via a website, an app, a log-on account, the interface of an IoT device or by e-mail a digital signature of the consumer along with consent details should be recorded which should be mapped with the data being processed. Which may be used by controller to prove that a data subject in a given case has provided his /her consent.

In practice, withdrawing consent should be as easy as obtaining it. The data subject must be able to withdraw consent via the same electronic interface, as switching to another interface would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means that a controller must make withdrawal of consent possible free of charge and without lowering service levels.

Implementation of a consent mechanism

To implement a consent mechanism, an organisation should base its execution on the architectural components defined above. The consent management framework, architecture and data model developed should enable a website or app to be compliant with the relevant regulatory requirements by prompting users for consent, collecting and managing that information, and passing the data to downstream partners. The following steps can be used to develop and implement an effective consent management platform:

Figure 3: Consent mechanism implementation steps



Analyse

Assess and analyse whether current consent practices are aligned with the privacy framework and identify any components that can be improved or added.

Design

Modify the existing consent practices and define new ones. Design templates to capture information for each component in the consent architecture.

Develop and implement

Develop interaction processes and model used between different components such as CM, DM and CH. Consider the differences between current privacy practices and the new ones that have been designed. Create an action plan to address these differences by implementing a tool which can support consent management processes and suggest training and support required by other employees to implement new or refined plans.

Operationalise

Continuously monitor consent management processes. Make necessary changes based on modifications to regulations and compliance policies/standards. Define report templates to support the reconciliation process in case of any audit or user query.

Changes/improvements required for effective consent management

Currently, most organisations which come under the purview of data protection laws and regulations such as GDPR, CCPA and India's proposed Personal Data Protection Bill are focused on defining advanced mechanisms for consent management to ensure compliance with these guidelines. However, organisation end up facing challenges to cope up with changing and dynamic regulatory landscape. Further, in the case of organisations which have to comply with more than one privacy law, consent is more difficult to manage.

To address these challenges, organisations should focus on:

- **Awareness:** Making people aware about changing consent management processes, what is changing, why it is changing, impact on employees, impact on clients/users, impact of not changing
- **Knowledge:** Providing information on privacy and consent processes and control rules
- **Ability:** Training to employees who collect consent (assessors), to management and others, as required

Along with the above improvements, organisations should design their consent-related processes in such a way that they are aligned with data management and governance processes and, at the same time, complement business processes.

Conclusion

Companies that wish to respect users' privacy and comply with various data protection regulations cannot create a transparent environment without consent collection. Unrestrained advertising and analytics with unlimited processing of user data – which have long been taken for granted – are now unethical and unlawful and will attract hefty penalties.

Collection of user consent is one of the pillars of lawful data processing and is essential for all marketing, advertising or any other type of promotional activity in which customer data is used. Implementing a consent management platform is the most sensible decision a business can take to stay on top of the changing and complex data protection and privacy compliance environment.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Bhopal, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai, Pune and Raipur. For more information about PwC India's service offerings, visit www.pwc.in

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Acknowledgements

This article has been researched and authored by Amit Lundia, Prakash Suman, Rajat Sharma and Ambrish Anand. Review and SME guidance was provided by Mukesh Deshpande.

Contact us

Mukesh Deshpande
Data Management Leader
Partner, Technology Consulting
mukesh.deshpande@pwc.com
+91 9845095391

Amit Lundia
Data Governance Leader
Director, Technology Consulting
amit.lundia@pwc.com
+91 9836922881

pwc.in

Data Classification: DC0

SG/December2019-M&C3710