भारतीय विशिष्ट पहचान प्राधिकरण

Unique Identification Authority of India

भारत सरकार

Government of India

Aadhaar Notice and Consent Guidelines

March 2022

AADHAAR

Mera Aadhaar, Meri Pehchaan

Purpose of this Document

This document entails guidelines which guides organizations and government departments leveraging Aadhaar and identity information on how to implement the notice and consent requirement for a comprehensive list of operational scenarios involving processing of personal data. This document is intended to be a comprehensive guide for implementing notice and consent in the Aadhaar context.

Audience

Any organization that processes Aadhaar number and identity information including Authentication User Agencies (AUAs) and e-KYC User Agencies (KUAs) may adopt these guidelines for implementing a standardized notice and consent requirement.

Disclaimer

Organizations adopting these guidelines should consult their legal experts prior to implementation of these guidelines to ensure that they understand the legal requirements and are compliant with the requirements of the various applicable laws once Notice and Consent requirement has been implemented. UIDAI disclaims all liability of any kind, whether express or implied, as to the results or benefits of implementing the guidelines.

Version Control

Version No.	Approver	Nature of Change
1.0	First Draft	

Table of Contents

1. Executive Summary

The concept of Notice and Consent are the founding principles of data protection and privacy and are significantly positioned in all the data protection laws across the world. In India, the Information Technology Act, 2000 and the Aadhaar Act, 2016 are the legislations that mention similar terms ("Disclosure of information" in Aadhaar Act and "Consent" in IT Act and Aadhaar Act) in context of processing "Personal Information" (IT Act) and "Identity information" (Aadhaar Act). The Personal Data Protection Bill, 2019 also underlines the importance of "Notice" and "Consent" for processing of personal data[1].

For organizations and Government departments there has been a constant challenge to comprehend and translate these legal requirements in order to implement the same through technology, systems and processes that would stand the test of the law. Further efforts also need to be made to address the unique challenges in Indian context such as the level of digital literacy and local languages.

These guidelines is to provide guidance on practical implementation for Notice and Consent to address the scenarios of all possible operational interactions that involve collection and processing of personal data for various types of organizations.

In the guidelines a comprehensive list of interaction media have been identified that an individual use to interact with various organizations and Government departments. These media have been listed below as:

- Physical medium where an individual interacts by filling a physical form
- Physical medium where individual performs transaction on his own
- Physical medium where there is no active interaction, but personal data is collected and processed
- Physical medium where an individual is assisted by another person in performing a transaction
- Electronic medium where an individual interacts through a website / mobile application / IoT device etc.
- Telephonic medium where an individual interacts via Call & SMS

[1] *"Personal Data" could mean and include data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and may include any inference drawn from such data for the purpose of profiling.*

These media help in identifying various unique challenges to communicate Notice and take Consent, effectively, of the individual in the given context. Based on these media, following guidance has been provided for various scenarios:

- Notice across various mediums of interaction
- Consent across various mediums of interaction
- Evidence to establish proof of Notice and Consent across various media

2. Requirement

The Notice and Consent requirement and its effective implementation has been a matter of concern and has been a topic for debate all across the globe.

Notice and Consent are the enabling means by which the organisations can collect and process personal data and in the absence of any guidance on the subject they face challenges some of which are listed below:

- **Organizations[2] and Government departments** that collect and process Aadhaar number and identity information / personal data **need guidance on how and where to post a legally valid notice**.
- Organizations and Government departments **need guidance on what electronic evidence may be maintained** for establishing notice or consent.
- There **are no practical guidelines, recommendations, and best practices that are available** in a form that an organization can simply follow instructions and implement a legally valid notice and consent.
- **Local challenges in Indian scenario** involving multiple languages, vulnerable people, and groups that are largely unaddressed.

[2] *Organizations here refer to any entity including the State, a company, any juristic entity or any individual, who collects and processes Aadhaar number and identity information.*

3. A Comprehensive – Notice and Consent Guidelines

A simple, practical and implementable Notice and Consent guidelines for Government departments and Organizations[3] that collect and process personal data, that is:

1. **Practical and implementable: Provides specific guidelines** on how to implement notice and take consent for a comprehensive list of transaction scenarios involving personal data processing across various government and organization functions.
2. **Acts as an all-inclusive guiding rule book** to assist government departments and organizations that collect and process personal data and are seeking guidance on implementing legally valid notice and consent.
3. **Addresses local challenges in** Indian scenario. Notice and consent best practices, implementation methods focuses on language challenges, vulnerable people and groups.

3.1 Notice and Consent

The terms Notice and Consent are often misunderstood to be one and mean the same. Although the implementation of both involve the same purpose and help achieve the same result, they are significantly different in terms of their applicability based on the legal requirement.

Notice

Notice is disclosure of information and presentation of terms for collection of personal data. Notice helps in achieving the transparency principle. A good Notice informs an individual of the following:

- The purpose
- The nature and categories of personal data
- Identity and contact details of data collector
- Contact details of the data protection officer
- Withdrawal of consent
- Basis of processing & source of collection

[3] *It is an assumption that the organizations and departments that are referring these guidelines have a valid legal basis for processing of Aadhaar number and identity information.*

- Grievance redressal
- Retention period
- Parties with whom data is being shared
- Cross-border transfer
- Right to file complaints

Consent

Consent is an indication of the data subject's wishes, by way of a statement or by a clear affirmative action, which manifests its agreement to process personal data. Consent helps in achieving the choice principle. A good consent meets the following objectives:

- Provides clear terms, choices and alternatives without recourse to inference from conduct in a context
- Free
- Informed
- Specific
- Clear
- Capable of being withdrawn

4. How Aadhaar ecosystem partners can implement these guidelines

Organizations and Government departments that collects and processes Aadhaar data (Aadhaar number and /or any other connected data) including Authentication User Agencies, e-KYC User Agencies and Aadhaar Offline Verification Seeking Entities, referring to these guidelines for implementing Notice and Consent within their environment may do so by following the steps given below:

a) **Identify the various points of collection and use of Aadhaar number and identity information**. One of the media provided in section 5 below should match the mediums of collection for ecosystems partners. The media listed in these guidelines are as follows:

- Physical medium where an individual interacts by filling a physical form *(For example, collection of Aadhaar number on a form)*
- Physical medium where individual performs transaction on his own*(For example, collection of Aadhaar number through a self-service kiosk etc.)*
- Physical medium where there is no active interaction, but personal data is collected and processed *(For example, collection of Aadhaar related data where there is no active interaction with the resident)*
- Physical medium where an individual is assisted by another person in performing a transaction *(For example, collection of Aadhaar number by an Operator/ Business Correspondent etc.)*
- Electronic medium where an individual interacts through a website / mobile application / IoT device etc. *(For example, collection of Aadhaar number using a website / mobile application / any other application platform)*
- Telephonic medium where an individual interacts via Call & SMS *(For example, collection of Aadhaar number using Call / SMS (such as IVRS or a text message) as a medium)*

b) **Implementation of 'Disclosure of information' requirement**: From the list of practices provided in section 7, identify the relevant scenario and most feasible and practice method for notice or disclosure of information and apply the same.

c) **Implementation of 'record of disclosure of information' or evidence**: From the list of evidences provided in section 9, identify the relevant scenario and the respective method to implement evidence or 'record of disclosure of information'.

d) **Implementation of 'consent' requirement**: From the list of practices provided in section 10, identify the relevant scenario and the respective method to implement consent.

e) **Implementation of 'record of consent'**: From the list of practices provided in section 11, identify the relevant scenario and the respective method to implement 'record of consent'.

f) **Model Notice and Consent Template:** Organizations may also refer to section 14 of these guidelines for a model notice and consent form template that can be leveraged and filled-in as per the use case specific to the organization.

5. Medium of Interaction for an Individual

To solve the problem of Notice & Consent it is important to consider all mediums an individual use to interact:

Medium of Interaction			Indicative Use Cases
	1 **Physical Medium – A physical form is filled**	**In this mode there is a physical interaction and a form is filled by the individual where personal data is provided by them.** **Examples** ***Filling a physical form*** *– Aadhaar Enrolment, Bank account, Insurance forms, Hotel Accommodation, Driving License, Public transport pass, School/College admission, Examination application, Job onboarding formalities, Hospital admittance, Voter registration, Municipal facilities like Birth Certificate, Death Certificate etc.*	
	2 **Physical Medium – A self-service mode**	**In this mode there is a physical interaction and individual does the transaction on a kiosk or any other medium by himself in a physical center. In the process personal data is also provided on the kiosk.** **Examples** ▶ *ATM Machine – Providing card number, Inputting PIN number, Mobile number (for additional services)* ▶ *Airport Kiosk – Name, PNR, Logs of Physical presence at the kiosk* ▶ *eVisa Kiosk, WIFI service Kiosks, Self-service Kiosk in a bank, Vending machines (collect phone number), Self-service ordering Kiosks, Self-service health Kiosks, Retail and Showroom Kiosks, Food court Kiosks.*	

Medium of Interaction

3 **Physical Medium – No active interaction**

In this mode there is a physical presence and automated personal data capture without explicit interaction with the individual.

Examples

- *CCTV monitoring, Face Recognition through public CCTVs.*
- *Voice/Video recording in a meeting.*
- *Automated monitoring through tools deployed for security on a computer – DLP, website monitoring, Keylogger.*

Indicative Use Cases

Medium of Interaction

4 **Physical Medium – Assisted mode**

In this mode there is a physical presence and a person is helping fill an electronic form on his device, in this process personal data is collected and filled in the application.

Examples

- *PDS subsidies distribution, Aadhaar based bank account opening through BCs.*
- *Cinema hall, Cafes and Restaurant, Hotel reservation (where physical form is not filled), Chemist shop, Retail chains (at billing), Supermarkets, Insurance agents, Bank branches, Telecom retailers (SIM issuance), Driving License appointment.*
- *Over the counter ticket sales (Airlines, trains), Passport office, VISA appointment, Police station etc.*

Indicative Use Cases

Medium of Interaction

5 **Internet - Websites, Mobile Applications**

In this mode individual goes to a website or mobile app on his device and does the transaction by themselves and provides personal data in the process.

Examples

- *Creating an account on social media site*
- *Account registration on websites / apps – Ecommerce, Banking, Tour & travels, OTT platform, Event registration, Fitness apps, Entertainment, Telemedicine, Messenger apps, Online Games (Web. Mobile – including sports fantasy leagues etc.), Banking and trading (Stocks & Shares), News Websites, Magazines subscription. Collaboration tools, Educations websites/apps, Job portals, Document repositories, Marketing apps, sites, Online FIRs etc.*
- *App installation, Ticket booking (train, flight etc.)*

Indicative Use Cases

Medium of Interaction

6 **Internet – IoT enabled devices**

In this mode individual is using an IoT device which is automatically capturing personal data and sending directly from the device to the server and user may not have any active interaction while data is being captured

Examples

- *Smart meters, Smart Fridge, Smart TV, Smart Home, Wearables, Smart appliances such as Fisheye camera, Fitness device & app, Smart AC, Heater etc., Smart Speakers, Smart city technologies, etc.*
- *Smart Automation, Smart Health apps, Smart Vehicles, IoT enabled devices*

Indicative Use Cases

Medium of Interaction

7 **Phone or SMS – Calling or sending SMS**

In this mode individual speaks on the phone to a government department or organization and personal data is captured over the phone interaction.

Examples

- *Call center operations – Survey calls, Customer complains etc.*
- *SMS based services*

Indicative Use Cases

6. Challenges in implementing Notice & Consent

There are various challenges across physical and online mediums that an organization face while implementing a valid consent and exhibiting a notice. These have been categorized in this section of the document.

6.1 Common Challenges

The common challenges observed in implementing notice & consent across media are:

- High level usage of legal terminologies in the notice text making it difficult to understand for common populace.
- Notice is unreasonably long making it highly inconvenient for the user to read the text.
- Notice does not match with the practices being followed by the organization w.r.t personal data processing.
- User is given no genuine choice or a clear / easy mechanism to opt-out / deny the consent.
- Service is denied if the user does not provide consent (even where service does not necessarily require use of certain personal data for providing basic services).
- Text of notice is not readable or is inaccessible to differently abled people.
- Notice (privacy policy etc.) is often hidden or not accessible to the common user base.
- Inadequate information, unreasonable or vague text of notice. Information such as personal data collection, storage and processing are not adequately covered in the notice text.
- By default, the assumption is that the user agrees and gives consent.

6.2 Medium specific challenges observed in implementation of Notice and Consent

1. Challenges faced in **Physical medium where a form is filled such as Website, Mobile Apps / Self Service (Kiosks based modes)**
    - Notice is not easily or prominently visible.
    - Notice and Consent are bundled with terms and conditions.
    - User is given no genuine choice or a clear/easy mechanism to opt-out /deny the consent.
    - User is not informed of their rights such as right to withdraw consent.
    - Often user is lured into give consent by using marketing tricks.

2. Challenges faced in **physical medium where there is no active interaction**
    - Inherently by nature, in this medium, there is no active interaction by the user before their personal data is collected and hence it is challenging to find a suitable way to capture the attention of the user and notify them of the personal data collection.
    - Inadequate information, unreasonable or vague text of notice.
    - Notices are not displayed in places prior to entering the area of interest (for e.g. area under CCTV recording).
    - Low level of awareness w.r.t user's right to view their CCTV footage.
    - CCTV recording without legally valid reasons.
    - Overarching notices, unreasonable storage duration.

3. Challenges faced in p**hysical medium – assisted mode**

- Operator controls the device and inputs the information for the user and hence there is no assurance that the notice has been understood by the user and an informed consent has been provided.
- Difficult to ascertain if the operator informed the user.
- Difficult to ascertain if the operator asked the user to tick the consent.
- Service may be denied in absence if the user denies to provide personal data.
- Problem in demonstrating evidence of an informed consent.
- Collection of personal data without explaining the consent to the user.
- User doesn't have access to the notice text to make an informed choice.
- User is given no genuine choice or a clear mechanism to opt-out /deny the consent.
- Local languages or language of choice of user are often not factored in.
- Low awareness level: Operators also don't understand the purpose of notice and importance of an informed consent.
- Notice and consent are bundled up with other terms and conditions.

4. Challenges faced in **SMS; Phone based interaction**

- User is often denied service if in case consent is not given.
- User is not provided with an informed choice (For example, a call centre agent, after the call informs the user that the call has been recorded for quality purposes without any affirmative user consent).

- Consent is often obtained immediately after notice, without giving reasonable time to the user to make an informed choice.

5. Challenges faced in **IoT based interaction**

- Inherently by nature, in this medium, there is no / limited active interaction by the user with the device while their personal data is collected and hence it is challenging to find a suitable way to capture the attention of the user and notify them of the personal data collection.
- Most IoT devices fail to explain to the user how they process their personal data.
- Most IoT devices do not explain to user how and where these devices store their personal data. Often times it is not clear whether the data is shared or hosted over cloud outside the geographical boundary of the user's country.
- Most IoT devices do not explain to user how to delete their data or request deletion.
- Inadequate information, unreasonable or vague text of notice.
- User is given no genuine choice or a clear mechanism to opt-out /deny the consent.

7. Practices for Notice across the various medium[4]

EDIUM	Notice Practices			Where can it be implemented *(Indicative)*		
Physical Medium – A Form is Filled	Separate prominent section in the form	Short notice with privacy policy link	Notice bundled under Terms and Conditions	*Banks*	*Hotels*	*Visitor Management*
				Hospitals	*Aadhaar Enrolment Form*	*Tour, Travels, VISA*
Physical Medium – Self Service	Check box / Button Click short notice	Notice Boards (prominent display)	Link to Privacy Policy / Notice	*Banking Kiosks*	*Airport Kiosks*	*Food Outlets*
				Visitor Management	*ATM Kiosks*	*Shopping Complexes*
Physical Medium – No Active Interaction	Prominent Sign Boards	Attention Seeking notice - In-Device Light / Blinker Notice	Privacy Policy	*Restaurants*	*Airports, Train Transit*	*Public Places*
				Cinema Halls	*Parking facilities*	*Companies Offices*

LEGEND

Most Comprehensive ← → Least Comprehensive

[4] *For a more comprehensive implementation, a combination of multiple notice practices can be implemented depending on the use case.*

MEDIUM	Notice Practices			Where can it be implemented *(Indicative)*		
Physical Medium – Assisted Mode	Notice message in SMS OTP pre-transaction	Notice message in SMS post-transaction	Automated voice recording from the device	*PDS*	*Hospitals*	*Banks*
				Visitor Management	*Hotels*	*Shopping Complexes*
				School, Colleges	*Telecom*	*Insurance Sector*
	Printed receipt with notice post transaction	Verbal Notice from operators		*Government Offices*	*Passport office*	*Airports, Train & Metro*
Website, Mobile Applications	Just in time notice	Notice presented through Chatbot (WhatsApp, Facebook etc.)		*eCommerce*	*Hotels*	*Social Media*
	Checkbox (tick/click) layered notice	Privacy Policy		*Hospitals*	*Matrimonial Sites*	*Education, Job Sites*
				Banks	*Tour & Travels*	*Insurance*

LEGEND

MEDIUM	Notice Practices			Where can it be implemented *(Indicative)*		
IoT Devices	In device buzz/blinking	Use of stickers, icons as notice on the device	Checkbox (tick/click) notice (For UI configured devices)	*Connected appliances*	*Smart Locks*	*Smart Refrigerator*
	Notice displayed within device	Privacy Policy		*Smart TV*	*Smart Meter*	*Smart Home*
				Smart Watch	*Smart Light*	*Smart Car*
SMS, Phone based interaction	IVR message with notice	SMS based notice		*Call Centers*	*Inbound SMS service*	

LEGEND

8. Legally admissible methods for establishing evidence for notice and consent

1. **Section 73** of the **Indian Evidence Act** provides the legal basis for admissibility of **signature** or **finger impression** in ink**.**

2. **Electronic Records**
    a. **Electronic record is defined under IT Act 2008** - As per the Act, electronic records include data, sound, image generated or recorded and sent or received in electronic form. Indian Evidence Act permits the admissibility of electronic records.
    b. **Admissibility of electronic record [Evidence Act] -** The contents of electronic records may be proved in accordance with the provisions of section 65B.

3. **Digital signature and Electronic signature is defined** under the IT Act 2000
    a. Section 3 of IT Act 2000 – Digital signature.
    b. Section 3A of IT Act 2000 – Electronic signature.
    c. Legal recognition of Electronic Signature - Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.



9. How to establish evidence for Notice

1 **Physical Medium – A Form is Filled** form is filled by the individual where personal data is provided by them.

S. No.	Notice Practice	Evidence	Systems/ Processes required to preserve evidence
1.	**Separate prominent section in the form**	The signed form wherein notice was provided to be preserved either electronically or physically and maintained with a traceable indexing scheme (i.e. unique form identifier) as evidence.	• Document Management System (DMS) (if the Physical from copy is stored). • Data Repository/Storage (if the forms are stored electronically such as scanned copies). • Logs generation system for time stamped logs generated during electronic storage. • Tamper proof logging and monitoring of DMS to ensure electronic record integrity.
	Notice bundled with Terms and Conditions		

	A short notice on the physical form, with a link to privacy policy hosted online	The signed form wherein the short notice was provided to be preserved either electronically or physically and maintained with a traceable indexing scheme (i.e. unique form identifier) as evidence. For privacy policy evidence could be in the form of a version controlled, duly approved and valid privacy policy hosted on the link mentioned in the form. Additionally, the applicable privacy policy version should also be mentioned on the physical form along with the URL where the policy is hosted. Electronic record in form of web application version control confirming the presence of the specific version of policy on that version of application. Web-server logs where the policy is hosted should also be maintained confirming the accessibility of policy on the internet.	• Document Management System (DMS) (if the Physical from copies are stored). • Data Repository/Storage (if the forms are stored electronically such as scanned copies). • Logs generation system for times tamped logs generated during electronic storage of the documents. • Tamper proof logging and monitoring of DMS to ensure electronic record integrity. • Application version control system for the web URL where the policy is hosted. • Document Version Control System to maintain version number of privacy policy. • Change management system to record changes in application or privacy policy.

2 **Physical Medium – Self Service**

In this mode there is a physical interaction and individual does the transaction on a kiosk or any other medium by himself in a physical center. In the process personal data is also provided on the kiosk.

S. No.	Notice Practice	Evidence	Systems/ Processes required to preserve evidence
2.	**Check box notice**	Kiosk runs with an application which has a version number. The notice text is also a part of the application source code deployed on the kiosk. For evidence purposes, electronic record of the text of notice embedded / present in the application code (mapped to application version) deployed in production at the time of transaction, to be maintained.	• Application Source Code Version maintenance system/software. • Logs generation system for time stamped logs generated during the kiosk usage. Notice text/version number should also be a part of the logs. • Tamper proof system for storage and maintenance of logs and to ensure electronic record integrity. • Change management procedure to record application level changes (including any change to notice text).
	Notice Boards (prominent display)	In this practice, a notice board would be displayed at a prominent place on/near the kiosk. The record of presence of this notice board kept in the form of a daily audit checklist will be an evidence in this scenario. Additionally, a robust evidence would also involve	• Duly approved policy stating the requirement of maintenance of a daily audit checklist. • Duly approved audit checklist. • Acknowledgement record of receipt of policy

		capturing photo of the kiosk with notice in display and maintain storage of this timestamp embedded photo on a daily basis.	and audit checklist by the staff/personnel responsible for maintaining the checklist. • Document management system / Electronic storage to preserve and store the daily audit checklist, Kiosk photograph with notice board. • Logs generation system for times tamped logs generated during electronic storage of the documents. • Tamper proof logging and monitoring of DMS to ensure record integrity. • A change management procedure to record changes in audit checklist, notice board etc.
	Link to Privacy Policy / Notice	For privacy policy evidence would be a version controlled, duly approved and valid privacy policy. The same needs to be maintained and preserved for evidence purposes. Preferably, the applicable privacy policy version should also be mentioned on the kiosk screen at the time of user interaction. Electronic record in form of web application version control confirming the presence of the specific version of policy on that version of application. Web-server logs where the policy is hosted should also be maintained confirming the accessibility of policy on the internet. A robust evidence would also include transaction log	• Application Source Code Version maintenance system/software. • Logs generation system for times tamped logs generated during the kiosk usage. Notice text/version number/privacy policy version number should be a part of the logs. • Tamper proof system for storage and maintenance of logs and ensure integrity of electronic record. • Change management procedure to record application level changes (including any

		containing the notice text displayed along with timestamp and other metadata.	change to privacy policy).

3 **Physical Medium – No active interaction**

In this mode there is a physical presence and automated personal data capture is taking place without explicit knowledge of the individualIn this mode there is a physical interaction and a

S. No.	Notice Practice	Evidence	Systems/ Processes required to preserve evidence
3.	**Attention Seeking notice - In-Device Light / Blinker Notice**	As there is no active interaction involved in this medium, it should be ensured that the device in use, acts in a manner that is not covert while capturing personal data. The evidence would be a record of the working functionality that clearly signifies if the device is on and capturing data or not. Record of proper working of blinker light etc. functionality should be captured through the logs generated by the device. Alternatively, the policy of the organization should mandate daily inspection (checklist based) of the device to ensure the mentioned notice functionality is operational. Acknowledgement record of receipt of policy and audit checklist by the staff/personnel responsible for maintaining the checklist. Evidence in the form of daily inspection report, photos with time stamp and signature shall be maintained. .	• Logs generation system for times tamped logs generated by the device during its usage. The status of in-device light/blinker notice/buzzing sound must be captured in the logs. • Policy mandating daily inspection and physical / electronic document management system to trace the electronic record • Tamper proof system for storage and maintenance of logs and to ensure integrity of the records
	Prominent Sign Boards	In this practice, a notice board would be displayed at a prominent place on/near the device capturing personal data. For evidence, duly approved policy stating the requirement of maintenance of a daily audit checklist and acknowledgement record of receipt of policy and	• Document Version Control system to store duly approved policy stating the requirement of maintenance of a daily audit checklist.

		audit checklist by the staff/personnel responsible for maintaining the checklist. In addition, the record of presence of this notice board kept in the form of a daily audit checklist will be an evidence in this scenario. A robust evidence would also involve capturing photo of the device with notice in display and maintain storage of this timestamp embedded photo on a daily basis.	• Duly approved audit checklist. • Document Management System to store/preserve acknowledgement record of receipt of policy and audit checklist by the staff/personnel responsible for maintaining the checklist. • Document management system / Electronic storage to preserve and store the daily audit checklist, Kiosk photograph with notice board. • Logs generation system for timestamped logs generated during electronic storage of the documents. • Tamper proof logging and monitoring of DMS to ensure integrity of the electronic record. • A change management procedure to record changes in audit checklist, notice board etc.
	Privacy Policy	Privacy policy in isolation as a notice practice is not recommended in this scenario. Privacy policy shall be in addition to the above-mentioned notice practices and not used as a standalone practice of notice. Electronic record in form of web application version control confirming the presence of the specific version of policy on that version of	• Application Source Code Version maintenance system/software where the privacy policy is hosted. • Tamper proof system for storage and maintenance of application / URL version control and logs where the policy is hosted, confirming the availability of the privacy

		application. Web-server logs where the policy is hosted should also be maintained confirming the accessibility of policy on the internet. Preferably, the applicable privacy policy version and URL where it is hosted should also be mentioned on the notice board displayed.	policy online and ensuring integrity of the electronic record. • Change management procedure to record application (URL where privacy policy is hosted) level changes (including any change to privacy policy).

4	**Physical Medium – Assisted Mode**	In this mode there is a physical presence and a person is helping fill an electronic form on his device, in this process personal data is collected and filled in the application.

S. No.	Notice Practice	Evidence	Systems/ Processes required to preserve evidence
4.	**Notice message in SMS OTP pre-transaction / post-transaction**	In this practice a SMS with notice and OTP (in case of pre-transaction notice) or an SMS with notice is sent to user's phone. For evidence, logs generated at the SMS gateway's end at the time of sending SMS to the user along with electronic record of application version control deployed in production with SMS functionality implemented along with log generated containing at the minimum the timestamp, notice text, user identifier while sending SMS to be preserved as evidence.	• SMS gateway (SMS sending functionality). • Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. • Document Version Control System to maintain version number of notice text. • Change management system to record changes in application or notice text. • Tamper proof system for storage and maintenance of logs and ensuring integrity of the electronic record.
	Verbal Notice from operators	In this practice, an operator will follow a pre-defined script to give verbal notice to the user. For evidence, the policy where requirement of verbal notice is mentioned needs to be preserved along with the acknowledgement record of receipt of policy and audit checklist by the	• Document Version Control system to store duly approved policy stating the requirement of giving verbal notice to the user at the time of transaction.

		operator responsible for providing verbal notice. The version-controlled script containing the notice provided by the operator to be preserved. A robust implementation would also involve notice boards displayed in addition to verbal notice and evidence be stored for the display notice as well, in the form of a daily audit checklist with sample transactions reviewed and a time stamped photo with notice board and operator at the point of transaction may be maintained.	• Maintenance and storage of duly approved notice script. • Document Management System to store/preserve acknowledgement record of receipt of policy by the operator responsible for providing verbal notice. • Document management system / Electronic storage to preserve and store the daily audit checklist, photograph with notice board (if notice board is also displayed). • Logs generation system for timestamped logs generated during electronic storage of the documents. • Tamper proof logging and monitoring of DMS to ensure integrity of the electronic record. • A change management procedure to record changes in notice script, notice board etc.
	Automated voice recording from the device	In the practice, the application has the functionality to read out the notice text to the user in preferred language. For evidence, the recording traceable through a version number, electronic record of application version control deployed in production having the recording	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. Notice text/version number/privacy policy

		functionality and logs generated when recording is played in the application containing at the minimum timestamp, recording script, system sound level, user identifier etc. along with other meta data to be preserved.	version number should be a part of the logs. • System to maintain and store recording script. • Tamper proof system for storage and maintenance of logs and to ensure integrity of electronic record. • A change management procedure to record changes in notice script, audio etc.
	Printed receipt with notice post transaction	In this practice, user is provided with a receipt post transaction, containing the notice text as well among the other details. For evidence, application functionality record for printing receipt (i.e. application version-controlled source code), logs generated at the time of receipt printing and printing receipt (operator copy) be preserved. A robust evidence would also involve ensuring a user-signed printed receipt is preserved either electronically/physically by the operator.	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. • Document Version Control System to maintain printed receipt. • Tamper proof logging and monitoring of DMS to ensure integrity of electronic record.

5 **Website, Mobile Applications**

In this mode individual goes to a website and mobile app on his computer and does the transaction by themselves and provides personal data in the process

S. No.	Notice Practice	Evidence	Systems/ Processes required to preserve evidence
5.	**Just in time notice**	In this practice a Just-in-time notice is shown to the user, as and when there is a requirement to capture personal data. For evidence, electronic record of application version control deployed in production with Just-in-time notice functionality implemented along with log generated containing at the minimum the timestamp, notice text, user identifier to be preserved.	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. • Change management system to record changes in application or notice text. • Tamper proof system for storage and maintenance of logs and to ensure integrity of electronic record.
	Privacy Policy	For privacy policy evidence would be a version controlled, duly approved and valid privacy policy. The same needs to be maintained and preserved for evidence purposes. Preferably, the applicable privacy policy version should also be mentioned on the user screen. Electronic record in form of web application version control confirming the presence of the specific version of policy on that version of application. Web-server logs where the policy is hosted should also be maintained confirming the accessibility of policy on the internet.	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. Notice text/version number/privacy policy version number should be a part of the logs. • Tamper proof system for storage and maintenance of logs and to ensure integrity of electronic record.

		A robust evidence would also include transaction log containing the notice text/version/privacy policy version along with timestamp and other metadata.	• Change management procedure to record application level changes (including any change to privacy policy). • Document Version Control System to maintain Privacy Policy, Notice text.
	Checkbox (tick/click) layered notice. / Notice presented through Chatbot	Here notice is presented to the user on the screen. For evidence, electronic record of the text of notice/ privacy policy embedded / present in the application code (mapped to application version) to be preserved. Version controlled documents such as privacy policy etc. referred to in the text to be preserved. A robust implementation would also involve generated transaction logs with notice text, timestamp, user identifier and other meta data.	

6 **IoT Devices**

In this mode individual is using an IoT device which is automatically capturing personal data and sending directly from the device to the server and user does not have any active interaction with the device and hence my not have the knowledge at all.

S. No.	Notice Practice	Evidence	Systems/ Processes required to preserve evidence
6.	**Notice displayed within device, use of stickers, icons as notice on the device/Buzzing sound to attract attention**	In this practice an in-device notice is shown to the user either electronically or through stickers/buzzing sound in device. For evidence: Record of the working functionality that clearly signifies if the device is on and capturing data or not. Record of proper working of blinker light etc. functionality should be captured through the logs generated by the device. Record of confirmation of stickers/notices pasted on the device at the time of packaging for dispatch in the form of audit checklist. Electronic record of the notice/ privacy policy embedded / present in the application code (mapped to application version) for in-device notice.	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. • Tamper-proof system to store logs to ensure integrity of electronic record. • Document Version Control System to maintain Privacy Policy, Notice text. • Product manual / device information guide describing the notice displayed / buzzing sounds and their meaning etc.

		Device manual guide.	
	Privacy Policy	For privacy policy evidence would be a version controlled, duly approved and valid privacy policy. The same needs to be maintained and preserved for evidence purposes. Preferably, the applicable privacy policy version along with the link to privacy policy or embedded short privacy notice should also be mentioned on the user IoT device and evidence be captured in the form of version-controlled device code. Electronic record in form of web application version control confirming the presence of the specific version of policy on that version of application. Web-server logs where the policy is hosted should also be maintained confirming the accessibility of policy on the internet.	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. Notice text/version number/privacy policy version number should be a part of the logs. • Tamper proof system for storage and maintenance of logs and to ensure integrity of electronic record. • Change management procedure to record application level changes (including any change to privacy policy). • Document Version Control System to maintain Privacy Policy, Notice text.
	Checkbox (tick/click) notice (For UI configured devices)	Notice presented to the user using a UI interface (app/website). For evidence, electronic record of the text of notice/ privacy policy embedded / present in the application code (mapped to application version) to be preserved. Version controlled documents such as privacy policy etc. referred to in the text to be preserved.	

7 **SMS, Phone based interaction**

In this mode individual speaks on the phone to a government department or organization and personal data is captured over the phone interaction

S. No.	Notice Practice	Evidence	Systems/ Processes required to preserve evidence
7.	**IVR message with notice**	In this practice a notice is given to the user using an IVR message. For evidence: Version of IVR message. Version control of the IVR software that plays the specific recording. Electronic record of IVR recording.	• IVRS functionality. • Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the IVRS call. • Document Version Control System to maintain version number of notice text. • Change management system to record changes in application or notice text. • Tamper proof system for storage and maintenance of logs and to ensure integrity of electronic record.
	SMS based notice	In this practice a SMS with notice and OTP (in case of pre-transaction notice) or an SMS with notice is	• SMS gateway (SMS sending functionality). • Application Source Code Version

		sent to user's phone. For evidence, electronic record of application version control deployed in production with SMS functionality implemented along with log generated at the SMS gateway and application containing at the minimum the timestamp, notice text, user identifier while sending SMS to be preserved.	maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. • Document Version Control System to maintain version number of notice text. • Change management system to record changes in application or notice text. • Tamper proof system for storage and maintenance of logs and to ensure integrity of electronic record.

10. Practices for Consent across the various mediums

MEDIUM	Consent Practices		Where can it be implemented *(Indicative)*		
Physical Medium – A Form is Filled	Signature in ink on the form	Finger Impression in ink on the from	*Banks*	*Hotels*	*Visitor Management*
			Hospitals	*Aadhaar Enrolment Form*	*Tour, Travels, VISA*
Physical Medium – Self Service	Button click (Check-box tick etc.)	Notice Boards (prominent display) – **implicit consent**	*Banking Kiosks*	*Airport Kiosks*	*Food Outlets*
			Visitor Management	*ATM Kiosks*	*Shopping Complexes*
Physical Medium – No Active Interaction	Notice Boards – **implicit consent**	Prominent Sign Boards – **implicit consent**	Privacy Policy – **implicit consent**	*Restaurants*	*Airports, Train Transit*	*Public Places*
				Cinema Halls	*Parking facilities*	*Companies Offices*
Physical Medium – Assisted Mode	Verbal Notice given by operators	Button click (Check-box tick etc.)	SMS/Email based OTP submission	*PDS*	*Hospitals*	*Banks*
	Notice message in SMS post-transaction – opt out option	Printed receipt with notice post transaction – signature on the receipt		*Visitor Management*	*Hotels*	*Shopping Complexes*
				School, Colleges	*Telecom*	*Insurance Sector*
				Government Offices	*Passport office*	*Airports, Train & Metro*

MEDIUM	Consent Practices			Where can it be implemented *(Indicative)*		
Website, Mobile Applications	Configurable opt-in/ opt-out Privacy Policy	Just in time notice – implicit consent	Checkbox (tick/click)	*eCommerce*	*Hotels*	*Social Media*
	SMS/Email OTP submission	Affirmative choice through Messenger chatbot		*Hospitals*	*Matrimonial Sites*	*Education, Job Sites*
				Banks	*Tour & Travels*	*Insurance*
IoT Devices	Configurable opt-in/ opt-out Privacy Policy	Use of stickers, icons as notice on the device		*Connected appliances*	*Smart Locks*	*Smart Refrigerator*
	Checkbox (tick/click) (For UI configured devices)	Opt-in / opt-out Notice displayed within device		*Smart TV*	*Smart Meter*	*Smart Home*
				Smart Watch	*Smart Light*	*Smart Car*
SMS, Phone based interaction	IVR message with notice & pressing of a key	SMS based affirmative response to a notice		*Call Centers*		*Inbound SMS service*

11. How to establish evidence for consent

1 **Physical Medium – A Form is Filled**

In this mode there is a physical interaction and a form is filled by the individual where personal data is provided by them.

S. No.	Consent Practice	Evidence	Systems/ Processes required to preserve evidence
1.	**Signature in ink on the form**	The signed form wherein notice was provided, and consent was taken either in the form of a Signature / thumb impression to be preserved either electronically or physically and maintained with a traceable indexing scheme (i.e. unique form identifier).	• Document Management System(DMS) (if the Physical from copies are stored); • Data Repository/Storage (if the signed forms are stored electronically such as scanned copies); • Logs generation system for timestamped logs generated during electronic storage; • Tamper proof logging and monitoring of DMS to ensure electronic record integrity.
	Finger Impression in ink on the from		

2 **Physical Medium – Self Service**

In this mode there is a physical interaction and individual does the transaction on a kiosk or any other medium by himself in a physical center. In the process personal data is also provided on the kiosk.

S. No.	Consent Practice	Evidence	Systems/ Processes required to preserve evidence
2.	**Button click (Check-box tick etc.)**	Kiosk runs with an application which has a version number. The notice text is also a part of the application source code deployed on the kiosk. Electronic record of the text of notice embedded / present in the application code (mapped to application version) deployed in production at the time of transaction and the log generated at the time of click of button/check-box (record of consent) by the user to give consent. Evidence: Tick/Checkbox action log, timestamp, identification of individual, Record of SMS/OTP (if leveraged).	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the kiosk usage. Notice text/version number should also be a part of the logs. • Tamper proof system for storage and maintenance of logs and ensure integrity of the electronic record. • Change management procedure to record application level changes (including any change to notice text).
	Notice Boards (prominent display)	In this practice, a notice board would be displayed at a prominent place on/near the kiosk. The record of presence of this notice board kept in the form of a daily audit checklist will be an	• Duly approved policy stating the requirement of maintenance of a daily audit checklist. • Duly approved audit checklist.

		evidence in this scenario. Additionally, a robust evidence would also involve capturing photo of the kiosk with notice in display and maintain storage of this timestamp embedded photo on a daily basis. **Implicit consent.**	• Acknowledgement record of receipt of policy and audit checklist by the staff/personnel responsible for maintaining the checklist. • Document management system / Electronic storage to preserve and store the daily audit checklist, Kiosk photograph with notice board. • Logs generation system for timestamped logs generated during electronic storage of the documents. • Tamper proof logging and monitoring of DMS to ensure electronic record integrity. • A change management procedure to record changes in audit checklist, notice board etc.
	Consent in the form of electronic signatures.	An electronic signature can include a "digital" signature on a consent document (such as using e-Sign) or an any other method permissible under section 3 and 3A of Indian IT act. Evidence here will be the digital signature on the form.	• Document management system to index and retain the document with digital signature. • Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the kiosk usage. Notice text/version number/privacy policy version number should be a part of the logs. • Logs generated at the time of affixing electronic signature on the form. • Tamper proof system for storage and

			maintenance of logs and to ensure electronic record integrity. • Change management procedure to record application level changes (including any change to privacy policy). •

3 **Physical Medium – No active interaction**

In this mode there is a physical presence and automated personal data capture is taking place without explicit knowledge of the individual

S. No.	Consent Practice	Evidence	Systems/ Processes required to preserve evidence
3.	**In-Device Light / Blinker Notice**	As there is no active interaction involved in this medium, it should be ensured that the device in use, acts in a manner that is not covert while capturing personal data. The evidence would be a record of the working functionality that clearly signifies if the device is on and capturing data or not. Record of proper working of blinker light etc. functionality should be captured through the logs generated by the device. **Implicit consent.**	• Logs generation system for timestamped logs generated by the device during its usage. The status of in-device light/blinker notice/buzzing sound must be captured in the logs. • Tamper proof system for storage and maintenance of logs and to ensure electronic record integrity.

	Prominent Sign Boards	In this practice, a notice board would be displayed at a prominent place on/near the device capturing personal data. The record of presence of this notice board kept in the form of a daily audit checklist will be an evidence in this scenario. Additionally, a robust evidence would also involve capturing photo of the device with notice in display and maintain storage of this timestamp embedded photo on a daily basis. **Implicit consent.**	• Document Version Control system to store duly approved policy stating the requirement of maintenance of a daily audit checklist. • Duly approved audit checklist. • Document Management System to store/preserve acknowledgement record of receipt of policy and audit checklist by the staff/personnel responsible for maintaining the checklist. • Document management system / Electronic storage to preserve and store the daily audit checklist, Kiosk photograph with notice board. • Logs generation system for timestamped logs generated during electronic storage of the documents. • Tamper proof logging and monitoring of DMS to ensure electronic record integrity. • A change management procedure to record changes in audit checklist, notice board etc.

	Privacy Policy	Privacy policy in isolation as a notice and consent practice is not recommended in this scenario. For evidence, Electronic record in form of web application version control confirming the presence of the specific version of policy on that version of application. Web-server logs where the policy is hosted should also be maintained confirming the accessibility of policy on the internet. Preferably, the applicable privacy policy version and URL where it is hosted should also be mentioned on the notice board displayed.	• Application Source Code Version maintenance system/software where the privacy policy is hosted. • Tamper proof system for storage and maintenance of application / URL logs where the policy is hosted, confirming the availability of the privacy policy online. • Change management procedure to record application (URL where privacy policy is hosted) level changes (including any change to privacy policy).

4 **Physical Medium – Assisted Mode**

In this mode there is a physical presence and a person is helping fill an electronic form on his device, in this process personal data is collected and filled in the application.

S.No.	Consent Practice	Evidence	Systems/ Processes required to preserve evidence
4.	**SMS/Email based OTP submission**	In this practice a SMS with notice and OTP (for affirmative consent) is sent to user's phone. For evidence, electronic record of application version control deployed in production with SMS functionality implemented along with log generated after OTP is provided by the user containing at the minimum the timestamp, notice text, OTP success-failure, user identifier etc. to be preserved.	• SMS gateway (SMS sending functionality). • Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. • Document Version Control System to maintain version number of notice text. • Change management system to record changes in application or notice text. • Tamper proof system for storage and maintenance of logs and to ensure integrity of electronic record.
	Verbal Notice from operators	In this practice, an operator will follow a pre-defined script to give verbal notice to the user. For evidence, Operator must keep records that include the time & date of the transaction, the name and date/ version of the notice script used, user consent (accept/deny), user identifier at their end in an electronic/physical manner. A robust implementation would also involve notice boards also displayed in addition to verbal notice and evidence be stored for the display notice as well, in the form of daily audit checklist.	• Document Version Control system to store duly approved policy stating the requirement of giving verbal notice to the user at the time of transaction. • Maintenance and storage of duly approved notice script. • Document Management System to store/preserve acknowledgement record of receipt of policy by the operator responsible

			for providing verbal notice. • Document management system / Electronic storage to preserve and store the operator kept records, photograph with notice board (if notice board is also displayed). • Logs generation system for time stamped logs generated during electronic storage of the documents. • Tamper proof logging and monitoring of DMS to ensure electronic record integrity. • A change management procedure to record changes in notice script, notice board etc.
	Notice message in SMS post-transaction – opt out option	In the practice, the SMS with notice along with transaction confirmation is sent to the user post completion of transaction. For evidence, electronic record of application version control deployed in production with SMS functionality implemented along with log generated at the time of sending SMS to the user. Where application opt out provision to be given and log of SMS based opt outs to be maintained.	• SMS gateway (SMS sending functionality). • Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage and tamper proof storage. • Document Version Control System to maintain version number of notice text. • Change management system to record changes in application or notice text.

	Printed receipt with notice post transaction	In this practice, user is provided with a receipt post transaction, having the notice text as well among other details. For evidence, application functionality record for printing receipt (i.e. application version-controlled source code), logs generated at the time of receipt printing and printing receipt (operator copy) be preserved. A robust evidence would also involve ensuring a user-signed printed receipt is preserved either electronically/physically by the operator.	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. • Document Version Control System to maintain printed receipt. • Tamper proof logging and monitoring of DMS to ensure electronic record integrity.

5	**Website, Mobile Applications**	In this mode individual goes to a website and mobile app on his computer and does the transaction by themselves and provides personal data in the process

S.No.	Consent Practice	Evidence	Systems/ Processes required to preserve evidence
5.	**Just in time notice**	In this practice a Just-in-time notice is shown to the user, as and when there is a requirement to capture personal data. For evidence, electronic record of application version control deployed in production with Just-in-time notice functionality implemented along with log generated containing at the minimum the timestamp, notice text, user's record of consent, user identifier to be preserved. User's affirmative action through click on "I agree" or "check box" on agreement shall be preserved as evidence.	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. • Change management system to record changes in application or notice text. • Tamper proof system for storage and maintenance of logs and ensure integrity of electronic record.
	Configurable opt-in/ opt-out Privacy Policy	For privacy policy evidence would be a version controlled, duly approved and valid privacy policy. The same needs to be maintained and preserved for evidence purposes. Preferably, the applicable privacy policy version should also be mentioned on the user screen. A robust evidence would also include transaction log containing the notice text/version/privacy policy version along with timestamp and other metadata. Log of user's affirmative action through click of a button or checking a box for agreement on the policy should be maintained as electronic record.	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. Notice text/version number/privacy policy version number should be a part of the logs. • Tamper proof system for storage and maintenance of logs. • Change management procedure to record application level changes (including any

			change to privacy policy). • Document Version Control System to maintain Privacy Policy, Notice text.
	Checkbox (tick/click) layered notice, Consent through Messenger chatbot	Notice presented to the user on the screen. For evidence, electronic record of the text of notice/ privacy policy embedded / present in the application code (mapped to application version)to be preserved. Version controlled documents such as privacy policy etc. referred to in the text to be preserved along with log generated at the time obtaining consent which includes along with notice text, timestamp, user identifier, user action for consent (accept, deny etc.) and other meta data. Log of user's affirmative action through click of a button or checking a box or chat logs for agreement on the policy should be maintained as electronic record.	

6 **IoT Devices**

In this mode individual is using an IoT device which is automatically capturing personal data and sending directly from the device to the server and user does not have any active interaction with the device and hence my not have the knowledge at all.

S.No.	Consent Practice	Evidence	Systems/ Processes required to preserve evidence
6.	**Notice displayed within device, Use of stickers, icons as notice on the device/Buzzing sound**	In this practice an in-device notice is shown to the user either electronically or through stickers/buzzing sound in device. For evidence: Record of stickers/notices on the device at the time of packaging in the form of audit checklist. Electronic record of the notice/ privacy policy embedded / present in the application code (mapped to application version) for in-device notice and tamper-proof log of user action on displayed notice (accept/deny) along with timestamp, user identifier and other meta data. Where policy is agreed upon through a UI, log of the affirmative action through click of a button or checking a box on agreement of policy should be maintained.	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. • Tamper-proof system to store logs. • Document Version Control System to maintain Privacy Policy, Notice text. • Product manual / device information guide describing the notice displayed / buzzing sounds and their meaning etc.
	Privacy Policy (within device or over email)	For privacy policy evidence would be a version controlled, duly approved and valid privacy policy. The same needs to be maintained and preserved for evidence purposes. Preferably, the applicable privacy policy version should also be mentioned on the user screen / IoT device and the display be logged for evidence purposes. A robust evidence would also include log containing the notice text/version/privacy policy version, user	• Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. Notice text/version number/privacy policy version number should be a part of the logs. • Tamper proof system for storage and

		action on displayed policy (accept/deny) along with timestamp and other metadata.	maintenance of logs. • Change management procedure to record application level changes (including any change to privacy policy). • Document Version Control System to maintain Privacy Policy, Notice text.
	Checkbox (tick/click) notice (For UI configured devices)	Consent is taken after notice is presented to the user using a UI interface (app/website). For evidence, electronic record of the text of notice/ privacy policy embedded / present in the application code (mapped to application version) to be preserved along with user action for consent (accept/deny). Version controlled documents such as privacy policy etc. referred to in the text to be preserved. A robust implementation would also involve generated transaction logs having the notice text, timestamp, user identifier and other meta data. Log of user's affirmative action through click of a button or checking a box for agreement on the policy should be maintained as electronic record.	

7	**SMS, Phone based interaction**	In this mode individual speaks on the phone to a government department or organization and personal data is captured over the phone interaction

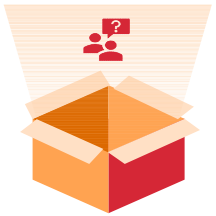
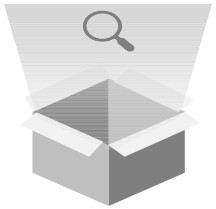
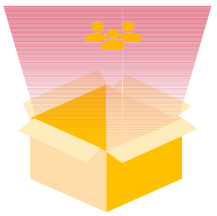
S.No.	Consent Practice	Evidence	Systems/ Processes required to preserve evidence
7.	**IVR message with notice & pressing of a key**	In this practice a notice is given to the user using an IVR message and consent is also obtained over IVRS. For evidence: Version of IVR message. Version control of IVR software with the specific message. IVR response / SMS response log, date, time stamp & identification of individual Electronic record of IVR recording. Log of User's affirmative action by pressing a key to choose the recording where explicit consent is required.	• IVRS functionality. • Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the IVRS call. • Document Version Control System to maintain version number of notice text. • Change management system to record changes in application or notice text. • Tamper proof system for storage and maintenance of logs and ensure integrity of electronic record. •
	SMS based affirmative response to a notice	In this practice a SMS with notice and OTP (in case of pre-transaction notice) or an SMS with notice is sent to user's phone and consent is obtained either in form of OTP or via SMS response. For evidence, electronic record of application version control deployed in production with SMS functionality implemented along with log generated containing at the minimum the timestamp, notice text, user identifier, user action on SMS text for consent while	• SMS gateway (SMS sending functionality). • Application Source Code Version maintenance system/software. • Logs generation system for timestamped logs generated during the application usage. • Document Version Control System to maintain version number of notice text.

		sending SMS to be preserved. Log of user's affirmative action by responding through an SMS with the choice shall be preserved.	• Change management system to record changes in application or notice text. • Tamper proof system for storage and maintenance of logs and ensure integrity of electronic record.

12. Elements for a Valid Consent

Consent is one of the most critical parts of any data protection law. Obtaining consent is not a straightforward solution for any organization. In order to form a valid consent, there are some principles that organizations shall always keep in mind while they are in the process of implementing consent and processing personal data. These key principles are:

1. **FREE**, having regard to whether it meets the standard under section 14 of the Indian Contract Act, 1872.
2. **INFORMED**, no later than at the time of collection of the personal data.
3. **SPECIFIC**, having regard to whether the user can determine the scope of consent in respect of the purposes of processing.
4. **CLEAR/AFFIRMATIVE**, having regard to whether it is indicated through an affirmative action that is meaningful in a given context.
5. **WITHDRAW**, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

13. Selecting the best Notice and Consent practice across medium

MEDIUM	NOTICE	CONSENT					
Physical Medium – A Form is Filled	Notice bundled under Terms and Conditions	Signature/ Finger Impression in ink on the form	Free	Informed	Affirmative	Easily withdrawn	
	Separate prominent section in the form	Signature/ Finger Impression in ink on the form	Free	Informed	Specific	Affirmative	Easily withdrawn
Physical Medium – Self Service	Link to Privacy Policy / Notice	Button click (Check-box tick etc.)	Free	Informed	Affirmative	Easily withdrawn	

MEDIUM	NOTICE	CONSENT					
Physical Medium – Self Service	Check box notice	Button click (Check-box tick etc.)	Free	Specific	Informed	Affirmative	Easily withdrawn
	Notice Boards (prominent display)	Notice Boards (prominent display)	Free	Specific	Informed	Affirmative	
Physical Medium – No active interaction	Prominent Sign Boards	Prominent Sign Boards	Free	Specific	Informed	Affirmative	
	Privacy Policy	Privacy Policy	Free	Specific			

MEDIUM	NOTICE	CONSENT					
Physical Medium – Assisted Mode	Verbal Notice from operators	Verbal Notice given by operators	Free	Specific	Informed	Affirmative	
	Automated voice recording from the device	Button click (Check-box tick etc.)	Free	Specific	Informed	Affirmative	Easily withdrawn
	Notice message in SMS OTP pre-transaction	SMS/Email based OTP	Free	Specific	Informed	Affirmative	Easily withdrawn
	Notice message in SMS post-transaction	Notice message in SMS post-transaction	Free	Specific	Easily withdraw		

MEDIUM	NOTICE	CONSENT					
Website, Mobile Apps	Privacy Policy	Opt-in/ Opt-out Privacy Policy	Free	Informed	Affirmative	Easily withdrawn	
	Just in time notice	Just in time notice	Free	Specific	Informed	Affirmative	Easily withdrawn
	Checkbox (tick/click) layered notice	Button click (Check-box tick etc.)	Free	Specific	Informed	Affirmative	Easily withdrawn
IoT Devices	Privacy Policy	Privacy Policy on the website	Free	Specific			

MEDIUM	NOTICE	CONSENT					
IoT Devices	Privacy Policy	Opt-in/Opt-out policy displayed via app	Free	Specific	Informed	Affirmative	Easily withdrawn
	Use of stickers, icons as notice on the device / sound	Use of stickers, icons on the device	Free	Specific	Informed	Affirmative	Easily withdrawn
	Notice displayed within device	Opt-in /Opt-out notice in device	Free	Specific	Informed	Affirmative	Easily withdrawn

MEDIUM	NOTICE	CONSENT	
SMS, Phone based interaction	IVR message with notice	IVR message with notice & pressing of a key	Free, Specific, Informed, Affirmative, Easily withdrawn
	SMS based notice	SMS based affirmative response to a notice	Free, Specific, Informed, Affirmative, Easily withdrawn

14. Model Notice and Consent

14.1 Model Notice

We, ***<Client Name>,*** are in the business of ***<add details of work>.*** We respect your privacy and handle your personal data in accordance with the applicable data protection laws. ***<Client Name>***may need to process your personal data for the purpose of ***<add details of the purpose>***in accordance with the provisions herein. This notice is intended to make you aware of the practices we follow regarding the data we collect, its use and protection.

Data we collect

We may collect and maintain certain personal data about you for***<add details of purpose>.*** The personal data collected may include but is not limited to:

<You may add Identity Information, Educational details, Professional Details, Health Information, etc.>

Purpose[s] of processing

We ***<Client Name>***keep and process information about you for ***<add details of the purpose>.*** The information may be used by ***<list all organizations that will use the information>*** for performing our key processing activities which includes:

<You may add the complete list of purposes for which personal data is being collected>

Sharing of personal data

We may share your personal data with ***<add details such as processors, vendors, business associates, service providers, etc.>***or where required or permitted by law.

Transfer of personal data

We may transfer your personal data to countries outside India. We will transfer personal data only for the purposes described above and in accordance with the applicable laws.

Retention of personal data

All personal data processed is stored and retained in compliance with legal, regulatory and best-practice business requirements. Your personal data will be collected, stored and processed till ***<add the timeline for purpose to be achieved>***. As soon as ***<add details of the purpose>***is achieved, we will securely delete/destroy your personal data as soon as practicable and in line with our data retention policies.

Rights of data subject

We acknowledge that you have a right to:

1. Access your personal data and related activities
2. Rectify your personal data
3. Erase your personal data
4. Restrict / object to processing of your personal data
5. Register a complaint

Security

We keep all data in secured servers in order to protect your personal data and have implemented industry standard security measures to keep our systems and premises secure. The security measures implemented include:
<You may include details about Limited access, Disciplinary action, System security, Logs, Audit Trails, CCTV, etc.>

Contact Grievance Officer

If you have any concerns as to how your data is processed, you can contact our Grievance Officer at ***<add details of the officer such as Name, Phone Number, E-Mail ID, etc.>***

14.2 Model Consent

By signing this Consent Form, you confirm that you have read the Privacy Notice hereunder and that you provide your unconditional consent to ***<Client Name>***for collecting and processing your personal data for the purposes mentioned therein. In the interest of complete disclosure, you can also consent to a limited number of purposes as listed herein. Also, please note that you can withdraw your consent to all or any of the purposes at any time by ***<add mode of withdrawal of consent>***. If you withdraw consent to such processing, we will stop processing your personal data however, any personal data already been processed shall remain unaffected by your withdrawal of consent.

Privacy Notice

We, ***<Client Name>,*** are in the business of ***<add details of work>.*** We respect your privacy and handle your personal data in accordance with the applicable data protection laws. ***<Client Name>***may need to process your personal data for the purpose of ***<add details of the purpose>***in accordance with the provisions herein. This notice is intended to make you aware of the practices we follow regarding the data we collect, its use and protection.

Data we collect

We may collect and maintain certain personal data about you for ***<add details of purpose>.*** The personal data collected may include but is not limited to:

<You may add Identity Information, Educational details, Professional Details, Health Information, etc.>

Purpose[s] of processing

We ***<Client Name>***keep and process information about you for ***<add details of the purpose>.*** The information may be used by ***<list all organizations that will use the information>***for performing our key processing activities which includes:

<You may add the complete list of purposes for which personal data is being collected>

Sharing of personal data

We may share your personal data with ***<add details such as processors, vendors, business associates, service providers, etc.>***or where required or permitted by law.

Transfer of personal data

We may transfer your personal data to countries outside India. We will transfer personal data only for the purposes described above and in accordance with the applicable laws.

Retention of personal data

All personal data processed is stored and retained in compliance with legal, regulatory and best-practice business requirements. Your personal data will be collected, stored and processed till ***<add the timeline for purpose to be achieved>***. As soon as ***<add details of the purpose>***is achieved, we will securely delete/destroy your personal data as soon as practicable and in line with our data retention policies.

Rights of data subject

We acknowledge that you have a right to:

1. Access your personal data and related activities
2. Rectify your personal data
3. Erase your personal data
4. Restrict / object to processing of your personal data
5. Register a complaint

Security

We keep all data in secured servers in order to protect your personal data and have implemented industry standard security measures to keep our systems and premises secure. The security measures implemented include:

<You may include details about Limited access, Disciplinary action, System security, Logs, Audit Trails, CCTV, etc.>

Contact Grievance Officer

If you have any concerns as to how your data is processed, you can contact our Grievance Officer at ***<add details of the officer such as Name, Phone Number, E-Mail ID, etc.>***

Signature:
Name:
Date:
Address:
Telephone:
Email:

15. Feedback and Suggestions

Feedback and Suggestions on the guidelines are solicited/invited/appreciated. We will include as many suggestions/feedback as possible in the future versions. It will help in enhancing/refining the guidelines further thus making the same more comprehensive and up to date with recent advancements in the field of notice and consent.

Address for Correspondence

Authentication Division, Unique Identification Authority of India

auth.regulations@uidai.net.in

Annexure A - Implementation of Notice across the various mediums

PressALT + Left Arrow Key to go back

Annexure A.1 Example of a form with notice bundled with other terms

- **Medium:**Physical Medium – A Form is Filled
- **Notice Practice:** Notice bundled under Terms and Conditions
- **Illustration:**Example of a VISA form with notice bundled with other terms

Some Key Points

- Take signature from user on the form.
- Recommended to leverage technology to store the signed consent form electronically and shared with user.
- Ensure form is in user's local language.
- Allow user with the option to provide thumb impression instead of signature.
- Provide the form in user's local language of choice.

Country Application Form For ABC Visa

This application form borne no cost

I am aware that visa fee is not refunded if the visa is refused.

Applicable in case a multiple-entry is applied for:
I am aware of the need to have an adequate travel medical insurance for my first stay and any subsequent visits to the territory of Member States.

I am aware of and consent to the following:

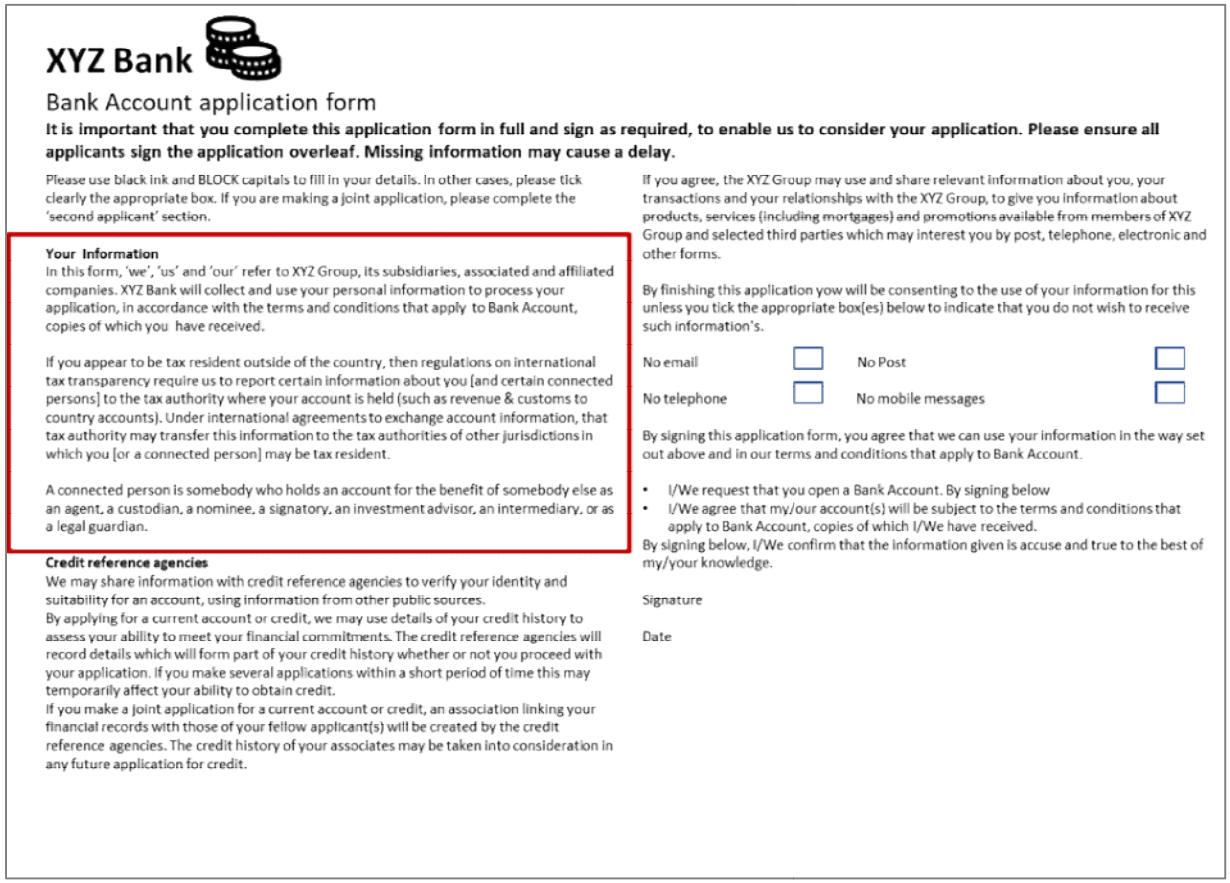
- the collection of the data required by this application form
- Capturing my photograph and, if applicable, capturing of fingerprints (for the examination of application)
- Any personal data concerning me which appear on the application form
- Fingerprints and my photography supplied and processed by the relevant authorities, for the purpose of decision on my application.

Such data as well as data concerning the decision taken on my application or a decision whether to revoke or extend a visa issued will be entered into to the system for a specified period, during which it will be accessible to the visa authorities and the authorities competent for carrying out checks on visas at external border and within the country, immigration for the purpose of verifying whether the conditions for the legal entry into, stay and residence on the territory of the country are fulfilled. Under certain conditions the data will be also available to the designated authorities for the purpose of prevention, detection and investigation of terrorist offences and of other criminal offences.

Annexure A.2 Example of a form with notice having a dedicated section

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – A Form is Filled
- **Notice Practice:**Separate prominent section in the form
- **Illustration:**Example of a Bank form with notice having a dedicated section



XYZ Bank

Bank Account application form

It is important that you complete this application form in full and sign as required, to enable us to consider your application. Please ensure all applicants sign the application overleaf. Missing information may cause a delay.

Please use black ink and BLOCK capitals to fill in your details. In other cases, please tick clearly the appropriate box. If you are making a joint application, please complete the 'second applicant' section.

Your Information
In this form, 'we', 'us' and 'our' refer to XYZ Group, its subsidiaries, associated and affiliated companies. XYZ Bank will collect and use your personal information to process your application, in accordance with the terms and conditions that apply to Bank Account, copies of which you have received.

If you appear to be tax resident outside of the country, then regulations on international tax transparency require us to report certain information about you (and certain connected persons) to the tax authority where your account is held (such as revenue & customs to country accounts). Under international agreements to exchange account information, that tax authority may transfer this information to the tax authorities of other jurisdictions in which you (or a connected person) may be tax resident.

A connected person is somebody who holds an account for the benefit of somebody else as an agent, a custodian, a nominee, a signatory, an investment advisor, an intermediary, or as a legal guardian.

Credit reference agencies
We may share information with credit reference agencies to verify your identity and suitability for an account, using information from other public sources.
By applying for a current account or credit, we may use details of your credit history to assess your ability to meet your financial commitments. The credit reference agencies will record details which will form part of your credit history whether or not you proceed with your application. If you make several applications within a short period of time this may temporarily affect your ability to obtain credit.
If you make a joint application for a current account or credit, an association linking your financial records with those of your fellow applicant(s) will be created by the credit reference agencies. The credit history of your associates may be taken into consideration in any future application for credit.

If you agree, the XYZ Group may use and share relevant information about you, your transactions and your relationships with the XYZ Group, to give you information about products, services (including mortgages) and promotions available from members of XYZ Group and selected third parties which may interest you by post, telephone, electronic and other forms.

By finishing this application yow will be consenting to the use of your information for this unless you tick the appropriate box(es) below to indicate that you do not wish to receive such information's.

No email ☐ No Post ☐
No telephone ☐ No mobile messages ☐

By signing this application form, you agree that we can use your information in the way set out above and in our terms and conditions that apply to Bank Account.

- I/We request that you open a Bank Account. By signing below
- I/We agree that my/our account(s) will be subject to the terms and conditions that apply to Bank Account, copies of which I/We have received.

By signing below, I/We confirm that the information given is accuse and true to the best of my/your knowledge.

Signature

Date

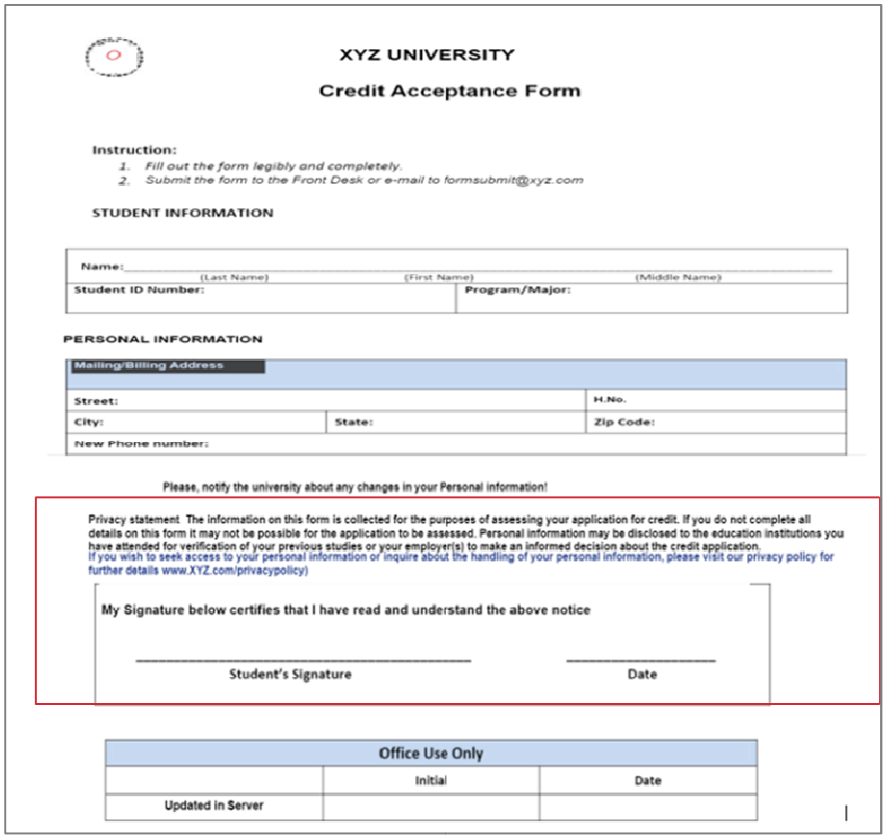
Some Key Points

- Take signature from user on the form.
- Recommended to leverage technology to store the signed consent form electronically and shared with user.
- Ensure form is in user's local language.
- Allow user with the option to provide thumb impression instead of signature.
- Provide the form in user's local language of choice.

Annexure A.3 Example of a form with short notice having link to privacy policy

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – A Form is Filled
- **Notice Practice:**Short notice with link to privacy policy
- **Illustration:**Example of a university form with short notice having link to privacy policy



XYZ UNIVERSITY

Credit Acceptance Form

Instruction:

1. *Fill out the form legibly and completely.*
2. *Submit the form to the Front Desk or e-mail to formsubmit@xyz.com*

STUDENT INFORMATION

Name: _____
(Last Name) (First Name) (Middle Name)

Student ID Number: | Program/Major:

PERSONAL INFORMATION

Mailing/Billing Address

Street: | H.No.

City: | State: | Zip Code:

New Phone number:

Please, notify the university about any changes in your Personal information!

Privacy statement The information on this form is collected for the purposes of assessing your application for credit. If you do not complete all details on this form it may not be possible for the application to be assessed. Personal information may be disclosed to the education institutions you have attended for verification of your previous studies or your employer(s) to make an informed decision about the credit application.
If you wish to seek access to your personal information or inquire about the handling of your personal information, please visit our privacy policy for further details www.XYZ.com/privacypolicy)

My Signature below certifies that I have read and understand the above notice

_____ Student's Signature

_____ Date

Office Use Only		
	Initial	Date
Updated in Server		

Some Key Points

- In this method a short notice is provided to the user with a privacy policy link included in the notice for detailed information.
- Take signature from user on the form.
- Recommended to leverage technology to store the signed consent form electronically and shared with user.
- Ensure form is in user's local language.

Annexure A.4 Example of a Kiosk application with link to its privacy policy as a means of notice

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – Self Service
- **Notice Practice:**Link to Privacy Policy / Notice
- **Illustration:**Example of a Kiosk application with link to its privacy policy as a means of notice

Some Key Points

- Default should not be YES.
- Summary of polices should be provided on the same screen to the resident instead of the links for better trust factor.
- Notice should be displayed prominently on the webpage and readable; allow local language of choice.
- Use clear, plain language that is easy to understand.
- Give an easy opt-out option.

Annexure A.5 Example of a Notice with a clear button click mechanism to opt-in or opt-out

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – Self Service
- **Notice Practice:**Button Click (Checkbox etc.) short notice
- **Illustration:**Example of a Notice with a clear button click mechanism to opt-in or opt-out

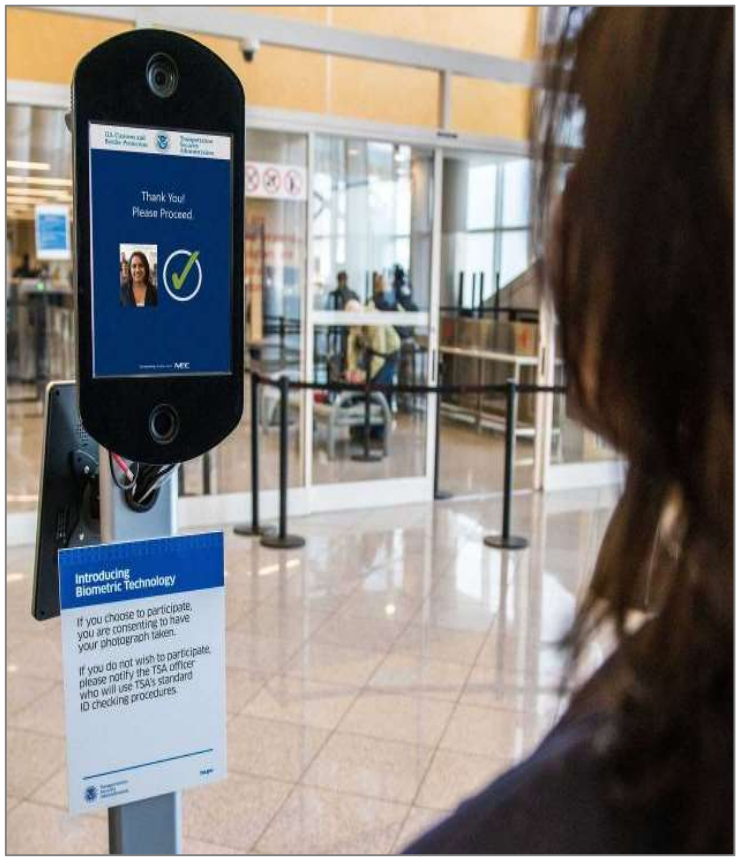
Some Key Points

- Default should not be YES.
- Recommended to not provide any default option, so that the resident makes a conscience choice.
- Notice should be displayed prominently on the webpage and readable; allow local language of choice.
- Use clear, plain language that is easy to understand.
- Give an easy opt-out option.
- include a separate consent form for each purpose.

Annexure A.6 Example of Face Recognition – Notice at Airports

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – Self Service
- **Notice Practice:**Notice Boards (prominent display)
- **Illustration:**Example of a Face Recognition – Notice at Airport



Some Key Points

- At the point of interaction, notice board is displayed
- Notice should be displayed prominently at the point of interaction and readable;
- Recommended to include notice in local language/ use of icons for better understanding
- Use clear, plain language that is easy to understand.
- Ensure there is no denial of service if not consented.

Annexure A.7 Example of anin-Device Light / Blinker Notice

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – No active interaction
- **Notice Practice:**LED lighting display (power on indicator) on the device while in use
- **Illustration:**Example of LED lighting display (power on indicator) on the device while in use

Some Key Points

- Clear notice in the form of LED lighting informing the user that the device is active and in use.
- Whenever the device is in use the indicator (power on indicator) should continue to remain on
- Functionality should be there to restrict any manipulation with the device switch on indicator

Annexure A.8 Example of Notice Board and Prominent Sign boards

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – No active interaction
- **Notice Practice:**Notice Board and Prominent Sign boards
- **Illustration:**Example of CCTV Recording Notices

Some Key Points

- **Use of color can have a significant impact** upon the **legibility of a notice**. Adequate contrast between the letters and their background can increase overall visibility and clarity of a message
- **Use the largest font size appropriate for the layout**, line length, and font characteristics. A **suggested size for body text is 10 or 11 point**, depending on the font weight, spacing, and line length (column width
- **Don't use more than two or three different fonts on the notice board.** Times New Roman for body copy and Arial for headings makes for a nice combination.
- **Don't place text on top of a picture; that makes it difficult to read.** The **use of abstract symbols should be minimized**and, where used, should be accompanied by a text component
- **Flush left, rag right text alignment is easiest to read** and should be used in most cases. Line length depends on the font's letter forms and point size selected.
- **Use hyphenation sparingly to avoid extremely long or short lines.** Avoid using more than two consecutive hyphenated lines.

PressALT + Left Arrow Key to go back

- **Body text and most display type should be set in Caps and Lower**- case. Reserve ALL CAP usage for short headlines or brief safety warnings
- **Avoid underlining**. Use italics, bold, or another type device for emphasis. If underlining must be used, make sure it does not touch the underlined letters.

Annexure A.9 Example of CCTV Privacy Policy

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – No active interaction
- **Notice Practice:**Privacy Policy
- **Illustration:**Example of CCTV Privacy Policy

Some Key Points

- Should be in addition to the notice boards.
- Have a dedicated privacy policy displayed on notice boards and/or websites/bills etc.
- In displaying the complete privacy policy is not possible, provide a short notice on the notice board and include link to the policy on the notice board.

XYZ Organization

Address

Contact: 011-2354-7691/7761 Email: xyz.organization.com

Policy Name	CCTV Policy & Procedure
Date Approved	DD-MM-YYYY
Date of Release	DD-MM-YYYY
Document Owner	Mr. Krishna Kumar

Introduction

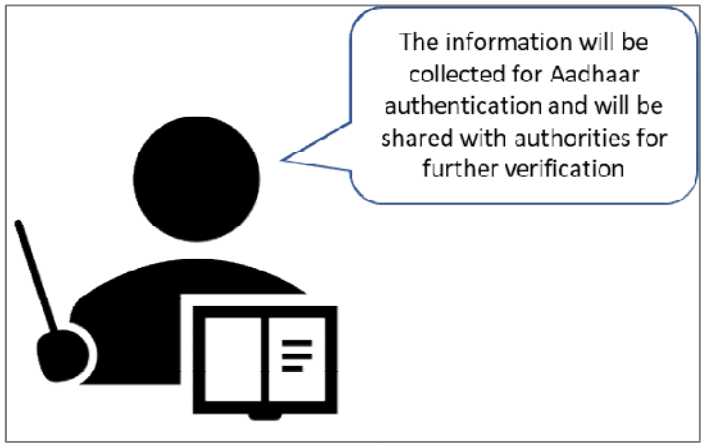
The purpose of this policy is to state how XYZ organization will deal with the requirement of law, particularly with Personal Data Protection Act, in respect of our use of the CCTV System at our regional office and headquarter.

All images will be monitored by the security department. Storage, collection and disposal will be adhered to the standard procedure defined by the organization and central government regulations in force.

Annexure A.10 Example of Verbal Notice / Display Notice

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – Assisted Mode
- **Notice Practice:**Verbal Notice / Display Notice
- **Illustration:**Example of a Verbal Notice / Display Notice



Some Key Points

- In addition to any other method – such as recording, physical form etc.
- Prominently display the notice at the entrance, counter, place of physical interaction.
- Trained operator who reads out and explain notice text to user.
- Notice should be displayed in local languages.

Annexure A.11 Example of Automated voice recording as notice practice

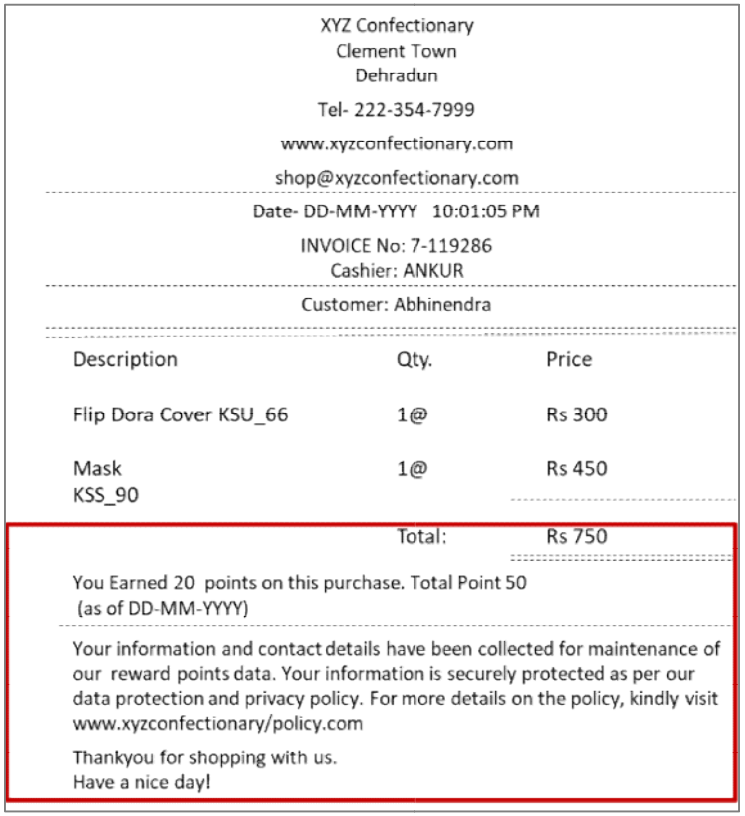
PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – Assisted Mode
- **Notice Practice:**Automated voice recording from the device
- **Illustration:**Example of Automated voice recording from the device

Annexure A.12 Example of Notice post transaction

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – Assisted Mode
- **Notice Practice:**Printed receipt with notice post transaction
- **Illustration:**Example of a printed receipt with notice post transaction



XYZ Confectionary
Clement Town
Dehradun

Tel- 222-354-7999

www.xyzconfectionary.com

shop@xyzconfectionary.com

Date- DD-MM-YYYY 10:01:05 PM

INVOICE No: 7-119286
Cashier: ANKUR

Customer: Abhinendra

Description	Qty.	Price
Flip Dora Cover KSU_66	1@	Rs 300
Mask KSS_90	1@	Rs 450
	Total:	Rs 750

You Earned 20 points on this purchase. Total Point 50 (as of DD-MM-YYYY)

Your information and contact details have been collected for maintenance of our reward points data. Your information is securely protected as per our data protection and privacy policy. For more details on the policy, kindly visit www.xyzconfectionary/policy.com

Thankyou for shopping with us.
Have a nice day!

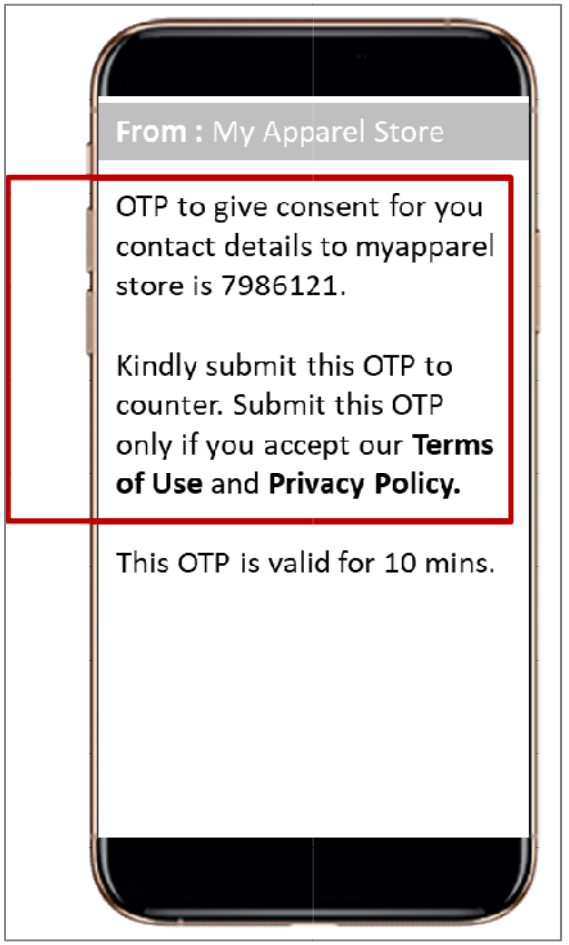
Some Key Points

- At the end of transaction, if a transaction slip/bill is generated, print the notice text on the bill.
- Store the copy of generated transaction slip along with notice digitally.
- Provide options to user to choose local language of their choice.

Annexure A.13 Example of Notice and Consent via SMS

PressALT + Left Arrow Key to go back

- **Medium:**Physical Medium – Assisted Mode
- **Notice Practice:**Notice and Consent via SMS
- **Illustration:**Example of SMS (OTP) based Consent



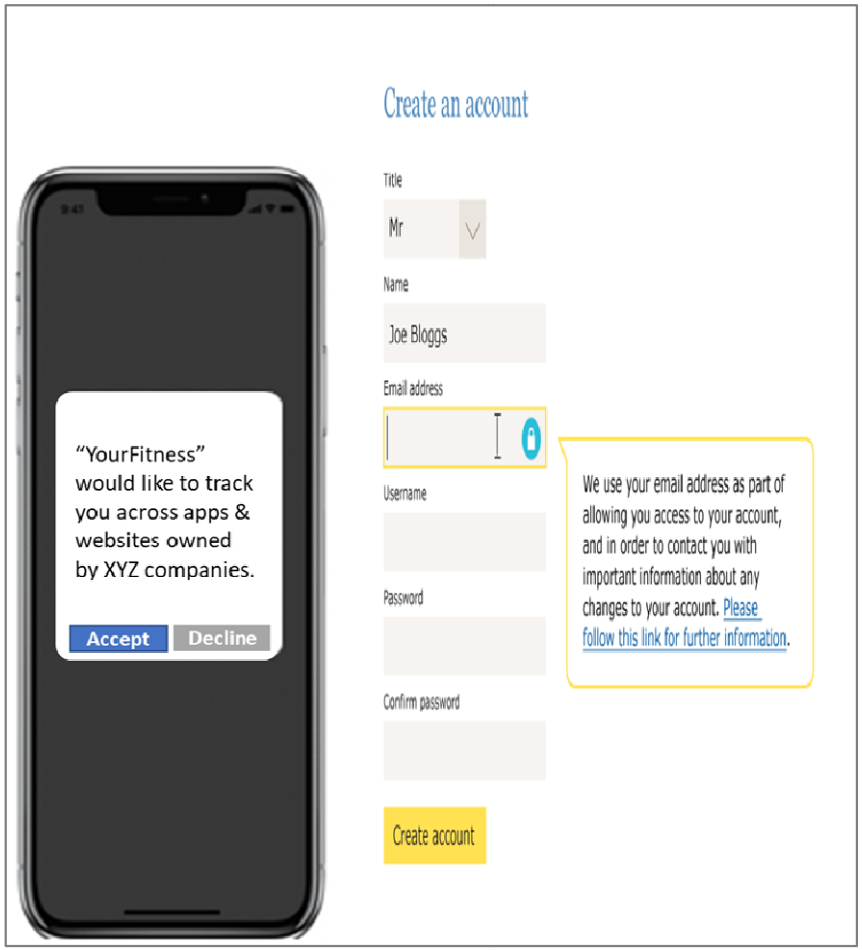
Some Key Points

- Notice text along with OTP is sent to user.
- User to read the text and provide OTP as consent.
- Allow resident to receive choose notice text in local language of choice.

Annexure A.14 Example of Just-in time notice

PressALT + Left Arrow Key to go back

- **Medium:**Website, Mobile Applications
- **Notice Practice:**Just-in time notice
- **Illustration:**Example of Just-in time notice



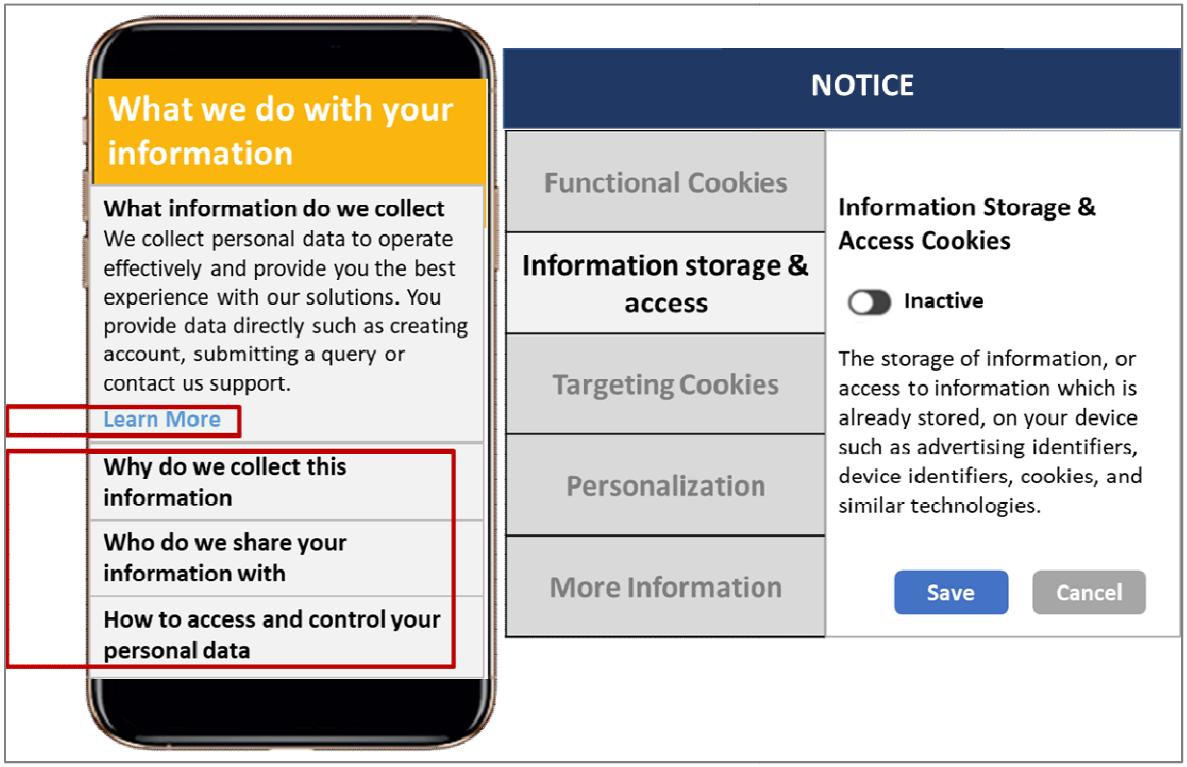
Some Key Points

- User is sent just –in-time notice text as popup.
- Just-in-time notices are sent to the user as and when they perform an action which requires their consent.
- Notices along with consent option are sent to the user.
- Also, apple through Just-in-time notice also allows for 'only once' consent.

Annexure A.15 Example of Checkbox Notice

PressALT + Left Arrow Key to go back

- **Medium:**Website, Mobile Applications
- **Notice Practice:**Checkbox Notice
- **Illustration:**Example of a Checkbox Notice



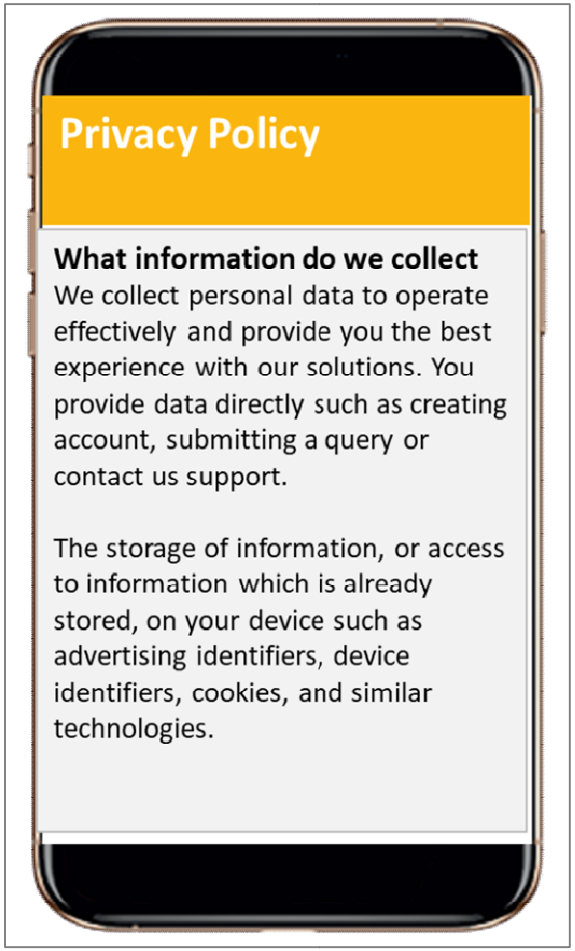
Some Key Points

- Display notice to the user at the time of interaction with website.
- Checkbox/Radio button implemented for consent.

Annexure A.16 Example of notice using Privacy Policy

PressALT + Left Arrow Key to go back

- **Medium:**Website, Mobile Applications
- **Notice Practice:**Privacy Policy
- **Illustration:**Example of a Privacy policy notice



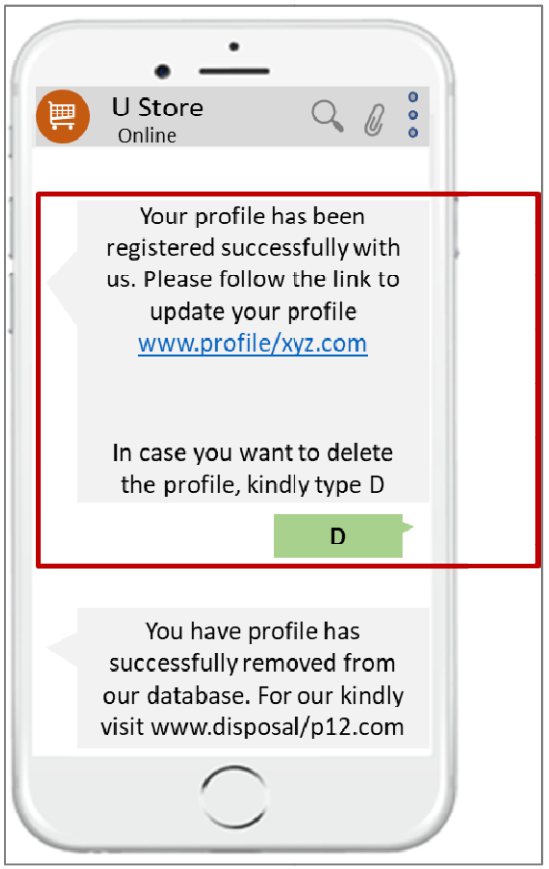
Some Key Points

- Privacy policy should be displayed prominently on the webpage and readable; allow local language of choice.
- Use Clear concise headers in the privacy policy.
- Use clear, plain language that is easy to understand.
- Give an easy opt-out option.
- Include a separate consent form for each purpose.

Annexure A.17 Example of a Chatbot Notice via messenger

PressALT + Left Arrow Key to go back

- **Medium:**Website, Mobile Applications
- **Notice Practice:**Notice via Messenger
- **Illustration:**Example of a Notice via Messenger



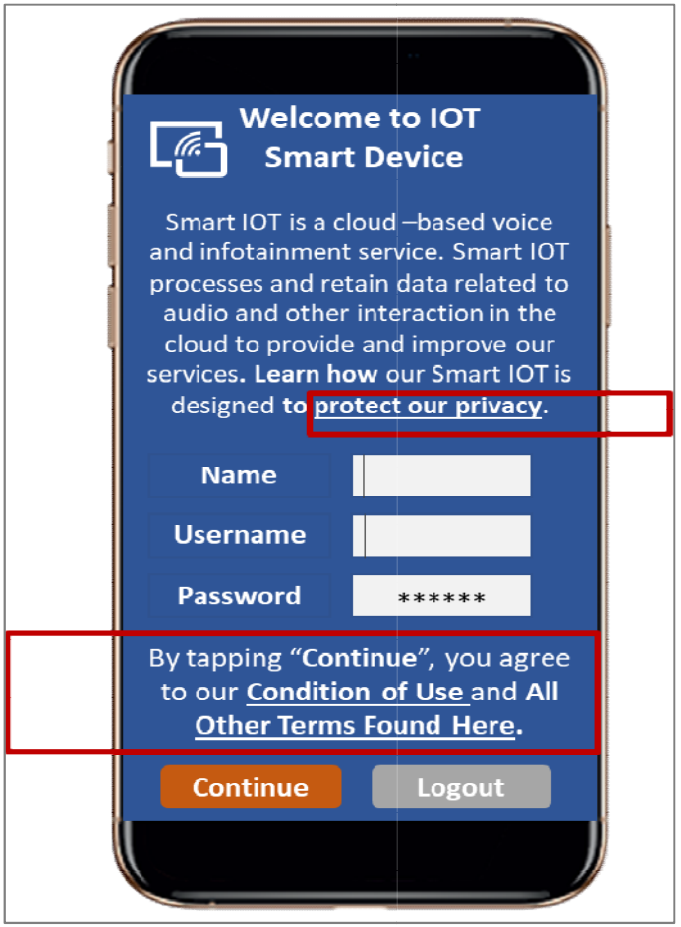
Some Key Points

- Send the notice text via messenger.
- Allow resident to give consent via reply to messenger text.
- Allow resident the option to choose local language.

Annexure A.18 Example of a Privacy Policy in the IoT device application

PressALT + Left Arrow Key to go back

- **Medium:**IoT Devices
- **Notice Practice:**Privacy Policy, Checkbox (IoT Device)
- **Illustration:**Example of a Privacy Policy in the IoT device application



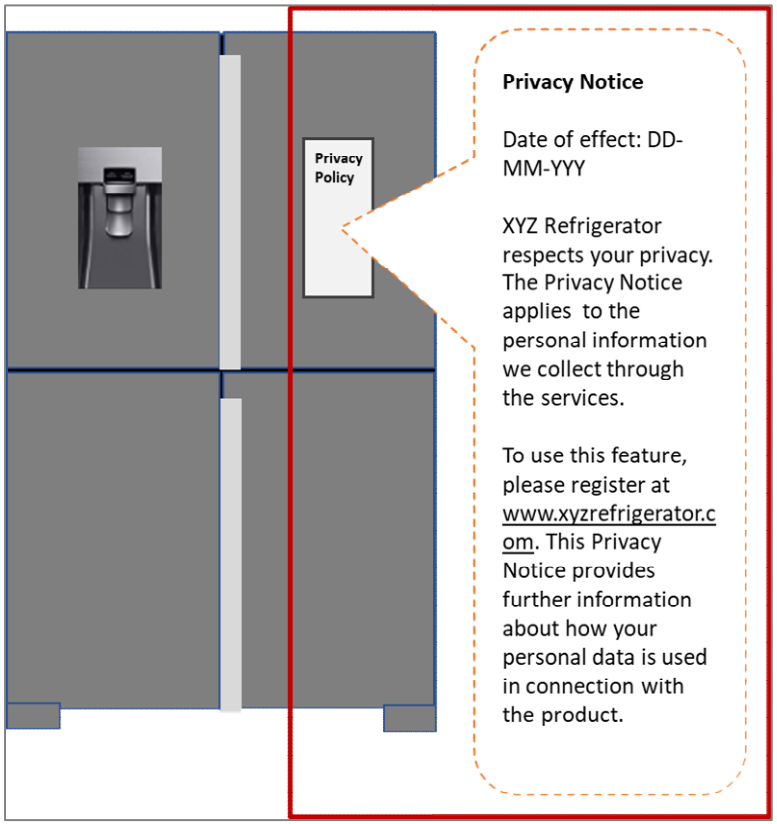
Some Key Points

- Display Privacy Policy to the user at the time of interaction with website.
- Checkbox/Radio button implemented for consent.

Annexure A.19 Example of a Notice displayed within IoT device

PressALT + Left Arrow Key to go back

- **Medium:**IoT Devices
- **Notice Practice:**Notice displayed within device
- **Illustration:**Example of a notice displayed within IoT device



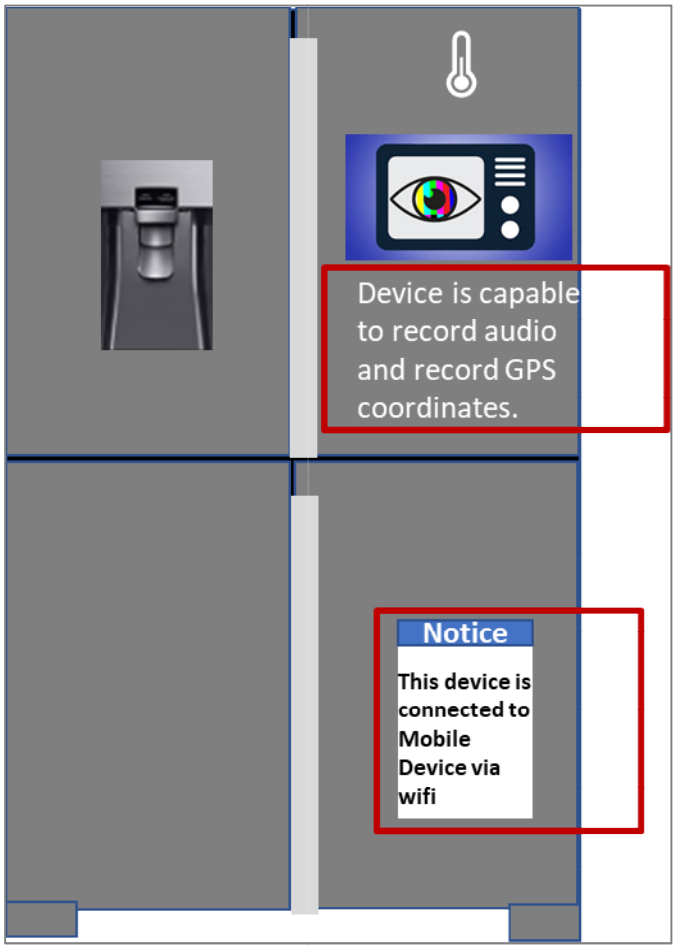
Some Key Points

- Display / make available notice the user within the device.
- User is provided the option to access the notice within the IoT device.
- Checkbox/Radio button implemented for consent.

Annexure A.20 Example of a notice displayed within the IoT device (Stickers / Icons)

PressALT + Left Arrow Key to go back

- **Medium:**IoT Devices
- **Notice Practice:**Notice displayed within device
- **Illustration:**Example of a Notice displayed within device



Some Key Points

- Display / make available notice the user within the device.
- User is provided the option to access the notice within the IoT device.
- Use of easily understandable icons.

Annexure A.21 Example of In-Device Buzzing / Blinker Notice

PressALT + Left Arrow Key to go back

- **Medium:**IoT Devices
- **Notice Practice:**In-Device Buzzing / Blinker notice
- **Illustration:**Example of LED lighting display (power on indicator) on the device while in use

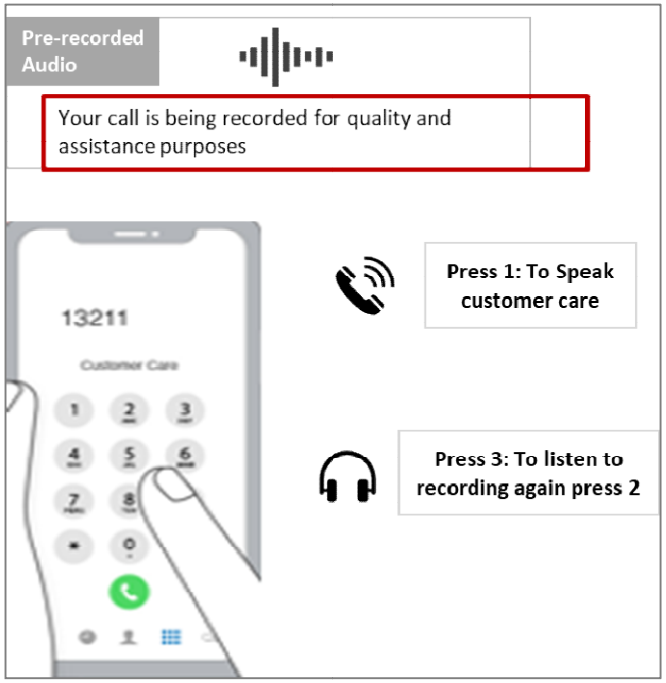
Some Key Points

- Clear notice in the form of buzzing sound / blinking light informing the user that the device is active and in use.
- Whenever the device is in use the indicator (power on indicator) should continue to remain on
- Functionality should be there to restrict any manipulation with the device switch on indicator

Annexure A.22 Example of IVRS Response Notice

PressALT + Left Arrow Key to go back

- **Medium:**SMS, Phone based interaction
- **Notice Practice:** IVRS Response (Notice via audio message)
- **Illustration:**Example of IVRS response notice



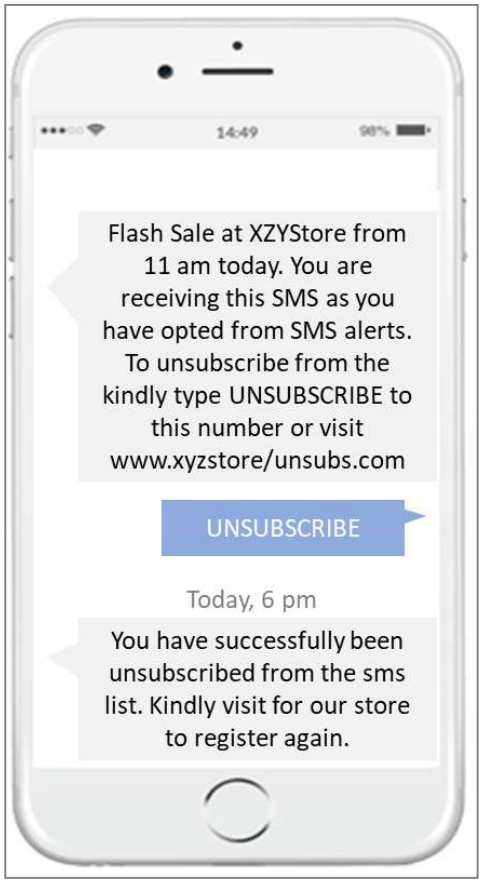
Some Key Points

- Automated readout of the notice text to user with the instructions to give or deny consent using keypress.
- Allow user the option to choose audio language.
- Allow user to hear consent message multiple times.
- Allow user to confirm through a key press.

Annexure A.23 Example of Notice via SMS

PressALT + Left Arrow Key to go back

- **Medium:**SMS, Phone based interaction
- **Notice Practice:** Notice via SMS
- **Illustration:**Example of Notice via SMS



Some Key Points

- Send the notice text via SMS.
- Allow resident to give consent via IVRS keypress or via SMS reply.
- Allow resident the option to choose audio and SMS text language.

Annexure B - Processing of personal data of children [Below 18 Years]

Processing of personal data of children [Below 18 Years]

The Children are more prone to the risks involved in the processing of Personal Data since they are less aware and easy to manipulate so they need extra protection when their data is collected and processed. The following pointers should be kept in mind while processing children's data:

- Organisations need to protect children from the manipulative design of the systems and processes
- Organizations must verify their age and obtain the consent of his parent or guardian
- Organisations must provide clear privacy notices for children to demonstrate how children's personal data is handled.

Methods of obtaining consent for processing personal data of children

1. **Parent Consent via email/SMS**
    a. Send email to parent's email address and seek consent over email.
    b. Ensure Parents email address is not provided by the child.
    c. Evidence: Electronic record of email.

2. **Parent Consent via telephone/video call**
    a. Have a customer service agent call on the parent's mobile and seek consent.
    b. Evidence: Call log and recording.

3. **Parent Signature upload and ID verification**
    a. Provide a copy of a form of government issued ID that you check against a database to verify age/relationship.
    b. Evidence: Transaction log of parent ID upload and verification

4. **Knowledge based challenge question [Approved by US FTC]**
    a. Send notice text email to parent's email with a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer.
    b. Evidence: Electronic record of email and electronic record of result of knowledge-based challenge

Unique Identification Authority of India

Bangla Sahib Road, Behind Kali Mandir, Gole Market, New Delhi – 110001

www.uidai.gov.in