

DPDP Compliance for NBFCs

A Webinar by:

FIDC
Finance Industry Development Council
(A Self Regulatory Organisation for NBFCs in India)

 **Consentin**
by Leegality

In Conversation With:



PUSHKAL DUBEY

Head of Consent Infrastructure

- Ex Privacy Lawyer at Trilegal
- Advised on global privacy regulations and the PDP Bill
- Product Manager building compliance products for BFSI
- Judge, NeGD 'Code for Consent: The DPDP Innovation Challenge'

Why do NBFCs need a privacy management tool?



NBFCs are data heavy.



Multiple touchpoints for data collection



Large scale third party involvement



DPDP compliance deadline-
13th May 2027

Whose personal data do NBFCs process?

- Customers
- Employees
- Guarantors / Co-applicants
- Nominees and Beneficiaries
- Individual contractors

What personal data do NBFCs process?

- **Identity Identifiers** like name, DOB, photograph
- **Government-Issued IDs** Aadhaar, PAN, VoterID
- **Financial and Income Records**
- **Credit History**
- **IP Address, location – device details**

KEY TIMELINES

Effective dates – Rule 1

- Data Protection Board – **Now**
- Consent Manager – **13th Nov 2027**
- Fiduciary obligations – **13th May 2027**
(18 month compliance window)

DPDP Act mandates a new era of transparency, trust and control

रजिस्ट्री सं० डी० एल—(एन)04/0007/2003—23

REGISTERED NO. DL—(N)04/0007/2003—23



भारत का राजपत्र The Gazette of India

सी.जी.-डी.एल.-अ.-12082023-248045
CG-DL-E-12082023-248045

असाधारण

EXTRAORDINARY

भाग II — खण्ड 1

PART II — Section 1

प्राधिकार से प्रकाशित

PUBLISHED BY AUTHORITY

सं० 25]

नई दिल्ली, शुक्रवार, अगस्त 11, 2023/ श्रावण 20, 1945 (शक)

No. 25]

NEW DELHI, FRIDAY, AUGUST 11, 2023/SRAVANA 20, 1945 (SAKA)

इस भाग में भिन्न पृष्ठ संख्या दी जाती है जिससे कि यह अलग संकलन के रूप में रखा जा सके।
Separate paging is given to this Part in order that it may be filed as a separate compilation.

MINISTRY OF LAW AND JUSTICE
(Legislative Department)

New Delhi, the 11th August, 2023/Sravana 20, 1945 (Saka)

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

(No. 22 OF 2023)

An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Seventy-fourth Year of the Republic of India as follows:—

Where to start?

First, let's see what a
consent journey looks like

Elements of a DPDP-compliant Consent Notice

Collect consent for each specific purpose.

The screenshot shows a mobile app interface for 'Consentin'. At the top, there's a navigation bar with 'Product', 'Customer & solutions', 'Resources', 'Pricing', and 'About'. Below this is a 'NOTICE' header with a language toggle (English/Hindi) and a close button. The main text states: 'We process your personal data only when necessary to provide you our banking services. By clicking on the "Accept all" button you give us your consent to process your personal data for the following purposes:'. Below this is a table with two columns: 'Purpose' and 'Data Categories'. The first row is 'Account Opening' (checked) with data categories: Name, Address, Aadhaar, PAN. The second row is 'Marketing' (unchecked) with data categories: Name, Email, Phone Number. Below the table, there's a link to manage consent in the preference centre. At the bottom, there are three buttons: 'Accept all', 'Accept selected', and 'Cancel', along with a download icon. A footer note says 'Secured by Leegality'. Red dashed arrows point from text annotations to specific UI elements: 'Collect consent for each specific purpose.' points to the table; 'Offer the option to choose preferred language' points to the language toggle; 'Clearly specify the data being captured' points to the 'Data Categories' column; 'Enables easy consent withdrawal and grievance redressal' points to the preference centre link; and 'Downloadable notice' points to the download icon.

Purpose	Data Categories
<input checked="" type="checkbox"/> Account Opening	Name Address Aadhaar PAN
<input type="checkbox"/> Marketing	Name Email Phone Number

Offer the option to choose preferred language

Clearly specify the data being captured

Enables easy consent withdrawal and grievance redressal

Downloadable notice

- **Clear:** Must be understandable independently and given in clear and plain language.
- **Vernacular Language:** The consent notice must be available in the languages in the 8th Schedule of the constitution.
- **Purpose & Data:** An itemised data categories mapped to purposes and goods and services must be there.
- **Means to Exercise Rights:** Withdrawing consent should be as easy as giving consent. It is ideal to provide links for the following in the consent notice:
 - Withdraw consent (with comparable ease).
 - Exercise rights under the Act.
 - Make a complaint to the Board.

PII Touchpoints Across NBFCs Flows

↑ Upstream Collection

- Website
- LOS
- Mobile Application
- Branch
- Business Correspondents
- Third-party Channel Partners
- Co-Lending Partners

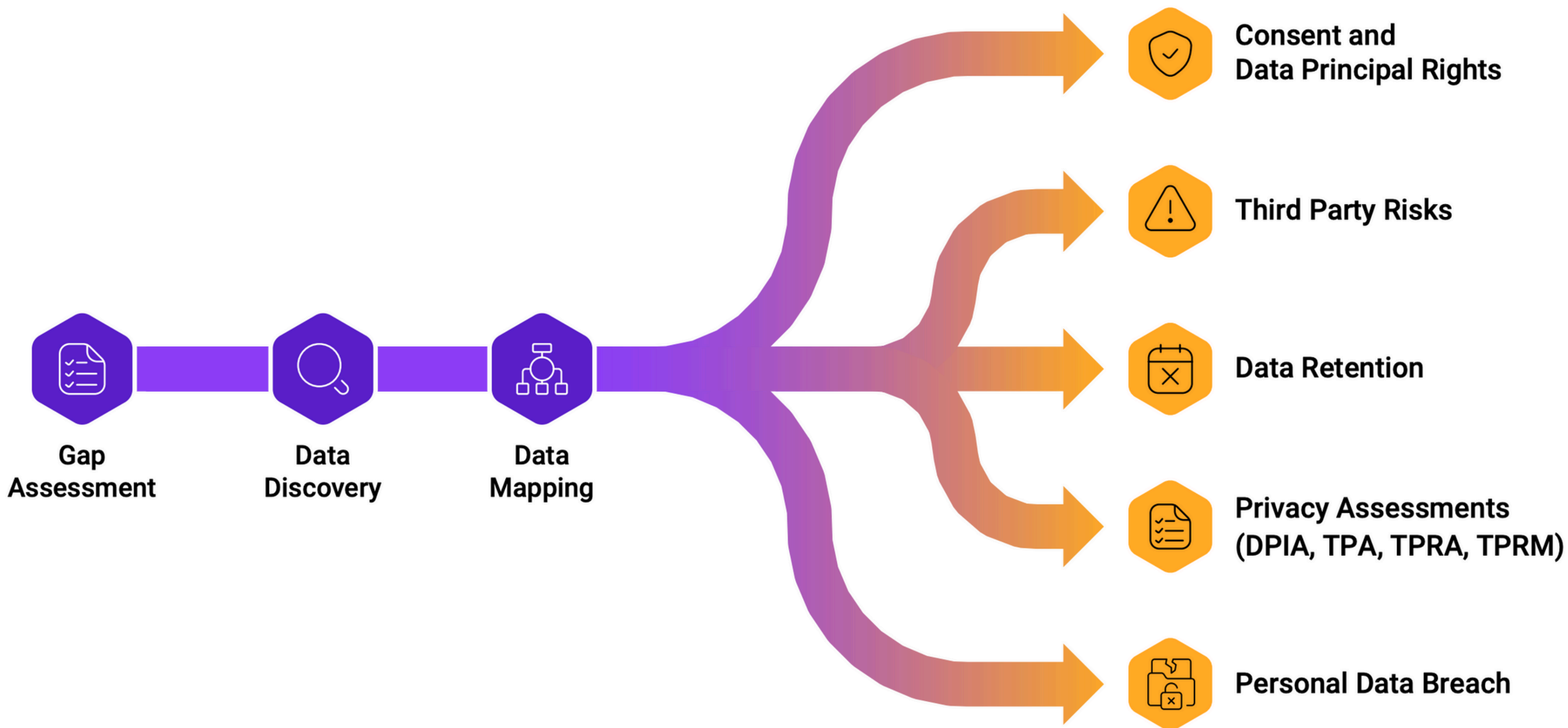


↓ Downstream Usage

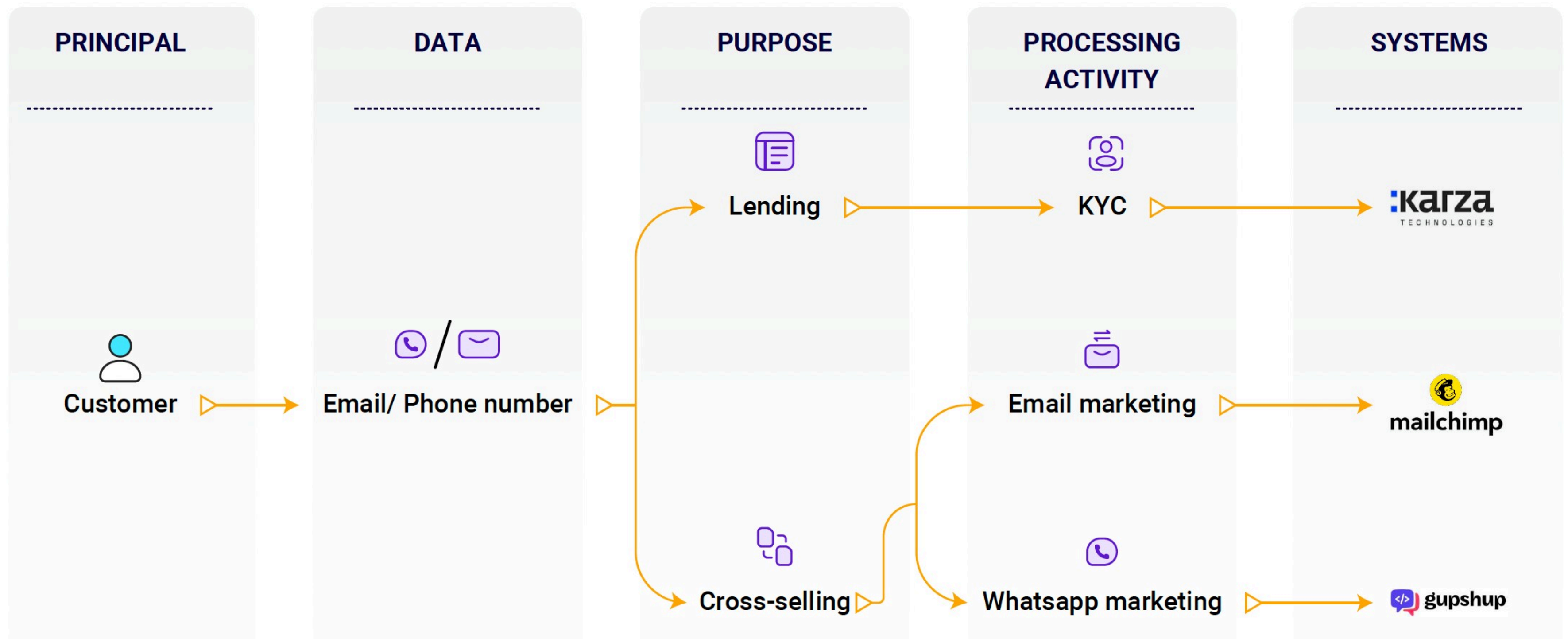
- Salesforce Financial Services Cloud
- Microsoft Dynamics 365 CRM
- Salesforce Marketing Cloud
- Snowflake
- MoEngage
- Power BI

How do you get here?

Data Protection Compliance Journey



Data mapping flow for an NBFC



The first step is to identify the data you process in your systems.

For this, you need to carry out data discovery.

What is personal data and how to find it?

Any data about an individual who is identifiable by or in relation to such data like, name, phone number, email id.


What to assess?	Examples
What systems do you use to process personal data?	Internal database, cloud storage, or third-party platforms
Is the data structured or unstructured?	Structured - mysql, postgres Semi Structure - json, xml Unstructured - google drive, emails
Data Identification and Categorization	Aadhaar, PAN, Phone Number etc.
Define sensitivity, control and risks	Aadhaar - Highly Sensitive Risks - Data Leak Controls - Encryption, tokenisation and data vault

This clarity is essential for compliance with privacy laws like the DPDP Act.

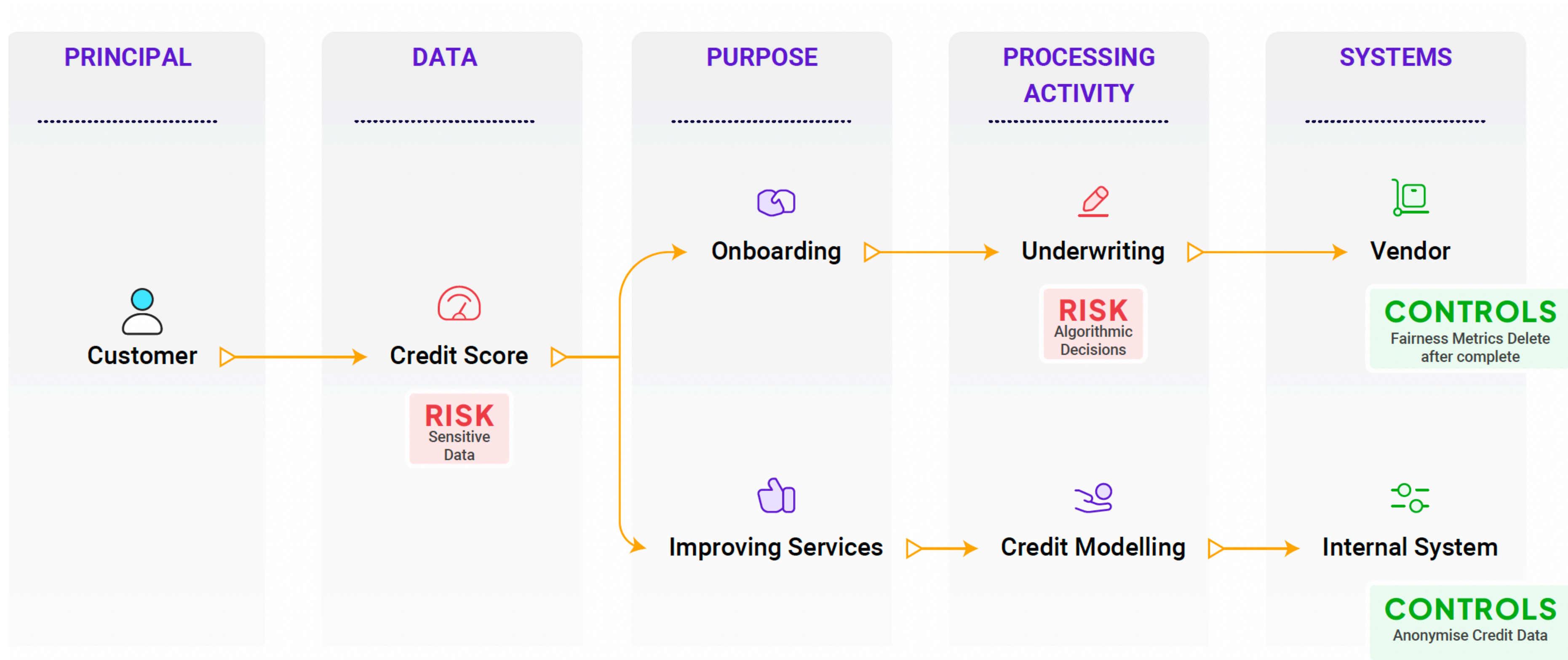
Once you know what data is in what system– you need to understand what you are doing with it.

For this, you need to carry out **Gap Assessments/DPIA**

The questions you need to answer

- 
- ✓ Are we collecting personal data?
 - ✓ Why are we collecting it?
 - ✓ How is it processed and stored?
 - ✓ Who do we share it with?
 - ✓ What controls exist (consent, retention, security)?
 - ✓ Whose data is it (customer/employee/vendor)?

Identify gaps through assessments



Ready to kickstart your compliance journey?

Scan the QR



or visit www.consentin.in