

PII Masking for High-Risk IDs

Aligning with Global Privacy Regulations

Protect Your Business with Automated PII Masking for High-Risk IDs

In today’s digital world, businesses collect sensitive customer data;

- Names
- Phone Numbers
- Email Addresses
- Payment Details

This Personally Identifiable Information (PII), is a high-value target for cybercriminals.

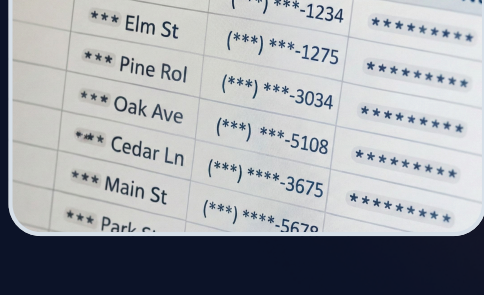
A data breach involving PII can lead to costly penalties, legal ramifications, and irreversible damage to customer trust.

Shufti’s PII Masking solution helps businesses secure their sensitive data by ensuring;

- ▶ Personal identifiers, such as national IDs, are masked.
- ▶ The masked data cannot be traced back to an individual.
- ▶ The data remains functional for internal use and compliance purposes.

Why This is Important for Your Business

Breaches involving sensitive data like Identification Number, Social Security Numbers (SSN), or Resident Registration Numbers (RRN) can lead to millions in penalties.



Global regulations like **GDPR**, **CCPA**, and **PIPA** are tightening the rules on handling and storing PII.

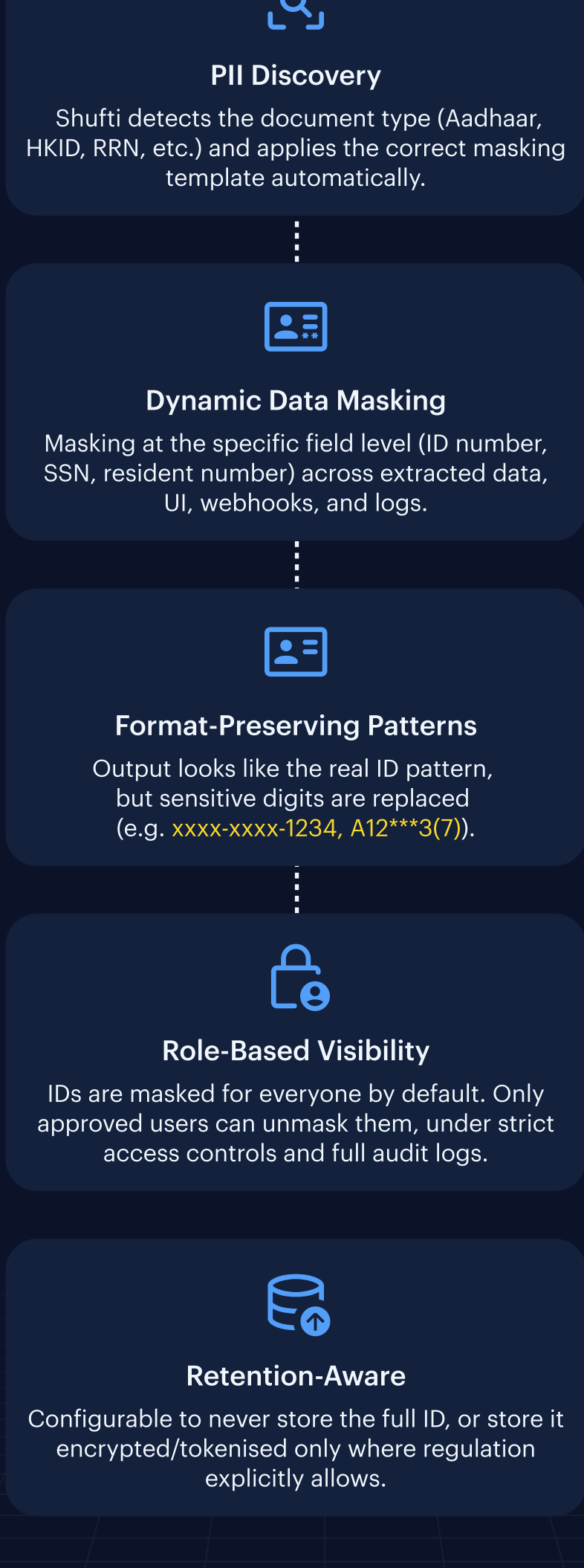
South Korea 🇰🇷 Under PIPA, full RRN usage is highly restricted, and the industry norm is to mask the last 6 digits.

Japan 🇯🇵 The My Number Act restricts full My Number disclosure.

Without masking, your business is at risk of unauthorized access and significant regulatory fines for non-compliance. Masking ensures that only authorized users can view sensitive data, reducing exposure and helping you avoid costly penalties.

How Shufti Handles PII Masking End-to-End

Shufti’s PII Masking Solution offers a comprehensive, automated approach to safeguard your sensitive data at every step.



Country-Specific Alignment Example

| Country / Region | Document Type | Masking Expectation | Shufti Implementation |
|------------------|---|---|--|
| 🇰🇷 South Korea | Resident Registration Card (RRN) | Full RRN usage highly restricted under PIPA; full number should not be stored or displayed except where explicitly allowed. | Treats RRN as high-risk PII: no persistence of full RRN by default; UI/API display YYMMDD-G***** (or stricter). |
| | Foreigner Registration Number | Industry norm: mask last 6 digits (e.g. YYMMDD-G*****). | Optional, tightly controlled unmasking where legally required. |
| 🇯🇵 Japan | My Number” (12-digit Individual Number) | My Number Act/ APPI: strict limits on collection/ disclosure; full number must not be shown except for specific legal purposes. Many orgs show only the last 4 digits internally. | Treats My Number as high-risk PII: default masking to last 4 digits or full tokenization; option to store raw number after verification. Unmasking restricted to specific roles/ flows with audit. |
| | My Number Card | | |

Why Choose Shufti?



End-to-End Data Masking

From collection to processing and storage, ensuring data is always protected.



Simplified Compliance

Our solution aligns with industry norms and regulatory expectations.



Reduced Regulatory Risk

By masking PII data, Shufti minimizes the chances of a breach and limits your exposure to fines and penalties (Stay compliant).




Audit-Ready


With Shufti, you have detailed logs of who accessed and unmasked data, making your business audit-ready at all times.

Stay ahead of regulatory requirements and protect your customers’ sensitive data with Shufti’s automated PII masking solution.

Request a Demo Today

To see how we can help you enhance your data security and compliance efforts.


www.shufti.com


sales@Shufti.com

Book a Demo