VARONIS

Indonesia Personal Data Protection Law

Contents

Overview

The Indonesia Personal Data Protection Law ("PDP Law"), enacted on October 17, 2022, regulates the collection, use, disclosure, and other processing of personal data by international organizations and governmental and private entities.

Similar to the EU's General Data Protection Regulation (GDPR), the PDP Law places different obligations on "Personal Data Controllers" ("Controllers") and "Personal Data Processors" ("Processors"). A Controller is a person, public agency, or international organization that acts individually or jointly in determining the purposes of and exercising control over the processing of personal data. A Processor is a person, public agency, or international organization that acts individually or jointly in processing personal data on behalf of a Controller.

The law imposes particular obligations on the processing of "Specific Personal Data" – which includes more sensitive categories of data such as health data, biometric information, and children's data – such as by requiring data protection impact assessments where a Controller processes Specific Personal Data.

The PDP Law sets forth responsibilities for organizations and privacy rights for individuals. It shares several concepts with other data protection laws, such as a requirement to process personal data only pursuant to a legal basis and an obligation to adopt policies and procedures to be accountable for compliance.

Additionally, the PDP Law requires Controllers to process personal data according to an enumerated set of processing principles, including that organizations must notify data subjects of the purposes for which they process personal data, must process personal data in a limited, specific, transparent, and lawful manner, and must protect the security of personal data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and loss.

The PDP Law applies to both organizations located within Indonesia and those located outside Indonesia, if the organization's data processing activities have legal consequences within Indonesia or affect Indonesian citizens outside of Indonesia. In this respect, the PDP Law has a broader scope of applicability than most other data protection laws, many of which only apply to activity within the country or directed to country residents.

Enforcement of the law begins in October 2024, two years after it was enacted. There are a variety of enforcement mechanisms under the PDP Law, including a private right of action for violations of the law, administrative fines, confiscation of profits or assets, and criminal penalties. The PDP Law provides for a Data Protection Authority to be established in order to administer the law and issue implementing regulations in the future.

Differences from GDPR

With the PDP law there are a few notable components unique to the Indonesian context. For instance, the PDP Law includes a broad exterritorial scope provision that will apply to organizations as long as their processing activities have legal consequences in Indonesia or cover Indonesian citizens outside of Indonesia.

Additionally, the PDP Law broadly exempts the financial services sector, imposes stricter requirements on Controllers such as broad record-keeping obligations for processing activities, and has unique provisions on the use of facial recognition technologies.

Special categories of data (what the PDP Law refers to as “specific personal data”) explicitly include children’s data and personal financial data. For specific data subject requests, such as access, rectification, and restriction, organizations only have 72 hours to respond.

PDP enforcement and fines

As for enforcement and sanctions, the PDP Law includes a large spectrum of avenues – from a private right of action for any violations of the law, to administrative fines and criminal penalties. For instance, the law sanctions “intentionally creating false data” with a criminal sentence of up to six years.

Administrative fines are mentioned briefly in the PDP Law, which states they will be determined by the PDP Agency and capped at a maximum of 2% of the offending entity’s annual income or revenue, depending on the severity of the violation.

Data-centric security

PDP regulations require companies to keep data privacy and data security requirements top-of-mind.

Knowing where sensitive data is and who can access it is a critical first step in ensuring data security. Once the organization has visibility into where sensitive data lives across different data stores and can determine who can access it and what they’re doing with it, they will then be able to identify where that data may be overexposed and when it might be compromised.

From a practical perspective, keeping data safe is nearly impossible without automation. Automation ensures companies can handle the scale at which data grows and the complexity of how that data should be managed. From a data security perspective, automation is a necessary approach for remediation.

In addition to automation, organizations also need continuous monitoring and alerting to detect cyberattacks and have a plan in place to respond to these attacks within the required timeframe.

Data is a company's most valuable asset. All it takes is one compromised user to gain access to data for an entire organization to be at risk. When companies watch data and eradicate excessive access, they make it harder for attackers, and easier to detect and stop early signs of compromise.

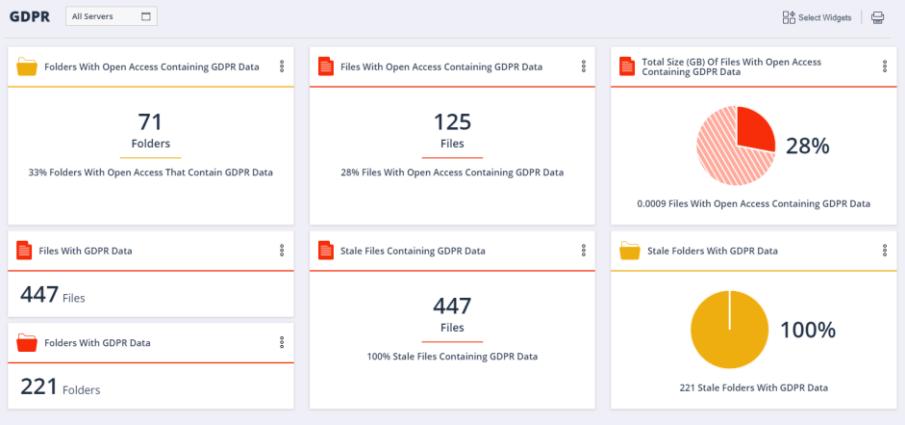
How Varonis can help

PDP-compliant data demands specific monitoring, policies, and processing. Once you discover and identify data susceptible to PDP regulations, you need to be able to secure and protect that data.

Discover and identify PDP data

The Varonis Data Security Platform can automatically discover where you have regulated PDP data across your critical data stores. These files can be Microsoft Word documents, spreadsheets, notepad files, even PDF files. Our Data Classification Engine is file-type agnostic and will find the data even if has been zipped.

Varonis has more than 540 global patterns, covering dozens of countries. Our platform identifies and flags data that looks like an IBAN number, social security number, passport number, personal ID card, facial recognition data, mobile phone number, license plate number, tax registry number, and more.



Varonis will continue to scan your data after the initial scan is complete since users will update and add data faster than you can lock it down. Varonis updates the previously mentioned folder and permissions map daily (or whatever you configure) and then adds modified folders back into the queue to get scanned again.

It's vital to maintain a holistic perspective of your PDP security status. Varonis provides several reports that allow you to keep track of your PDP data, which can be delivered to your inbox or a shared folder.

Under the PDP, individuals have rights to request and access the data a company maintains about them which must be provided "without undue delay and in any event within three days of receipt of the request." Fulfilling these requests manually can be a complex and time-consuming process.

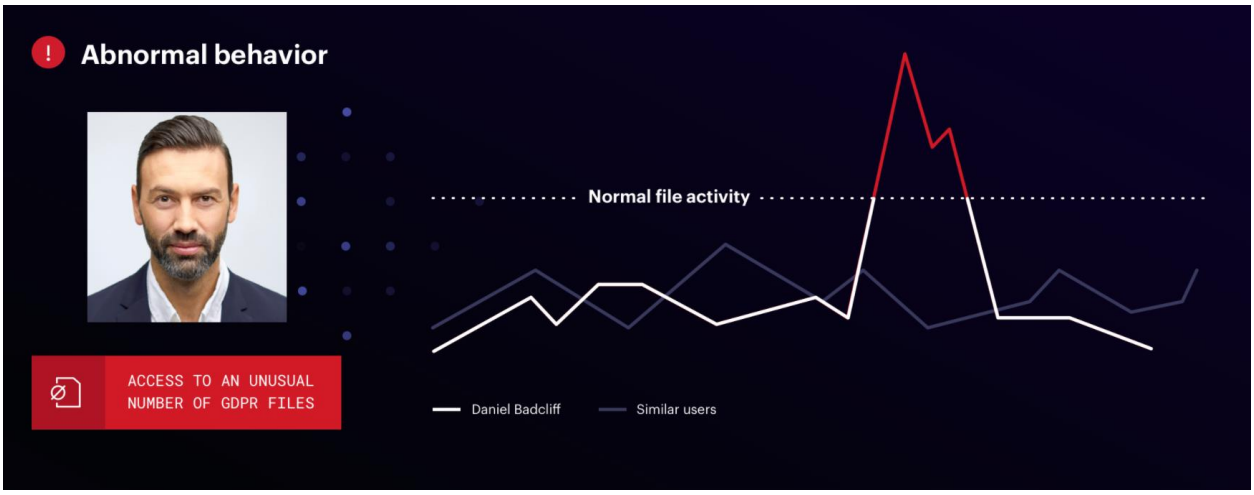
Varonis makes satisfying data subject access requests (DSAR) and complying with data discovery easier than ever before. Varonis surfaces personal information across cloud and on-prem files with a fast and powerful search. Our DSAR form uses sophisticated logic to ensure a company receives accurate results, avoiding false positives (and resulting fines).

Protect PDP data

Article 35 specifies security measures organizations must adopt to protect personal data, including preparing and implementing technical, operational measures and employing a risk-based approach to determine the level of appropriate security for data. Once access to data is limited, companies can then proactively protect PDP data by monitoring and analysing data activity and user behaviour and automating how to process that data.

Varonis applies data security analytics to file activity and user behaviour to highlight suspicious activity and unusual behaviour involving PDP data, streamlining investigations on potential threats. Varonis will also give you the heads-up needed to be able to report a data breach discovery within the PDP-mandated 72 hours.

As users create new files there is a possibility that PDP data will initially be left unsecured. Because Varonis is continuously scanning and discovering new PDP data in shares, it can move these newly discovered files containing PDP data to a quarantine folder. Once the PDP data is quarantined and secured, admins can investigate the file and determine who should have access, where it should be stored, and establish any additional conditions to help comply with PDP.



How Varonis maps to the PDP law security checklist

Indonesia's PDP law is the most wide-ranging, comprehensive piece of data privacy legislation in the country's history.

Here's how Varonis can help organizations achieve data security as expected by the PDP law:

PDP law checklist	How Varonis helps
Lawful Basis for Processing Personal Data:	
(Article 20) A controller of Personal Data shall have a basis for the processing of Personal Data, basis include: **a) explicit consent** **b) contractual obligation** **c) legal obligation** **d) vital interests** **e) public interest** **f) legitimate interest**	○ Controllers find Varonis' high-level risk dashboards and quantified granular reporting invaluable for prioritizing risk mitigation and evidencing good operational data privacy controls and processes. ○ Continually maps access across your hybrid environment, displayed within a single interface ○ Provides bi-directional view of access across all data platforms (who has access to what data and — unique to Varonis — what data does a group have access to) ○ Provides actionable recommendations on excessive access (over-permissive group members and unused permissions) ○ Allows for model changes in a sandbox environment to understand the impact before committing to the live environment ○ Rollbacks changes seamlessly ○ Automates reports directly to the data owner ○ Applies classification labels and encrypts files that have been identified as sensitive
(Article 21) In terms of processing of Personal Data based on approval as intended in Article 20 paragraph (2) letter a, Personal Data Controller is mandatory and must convey information regarding :	○ Create a visual map of your data estate—both on-premises and in the cloud—and identify who has access to it and whether they should have access

a. **Legality of the processing of Personal Data** b. **Purposes of processing Personal Data** c. **The type and relevance of the Personal Data to be processed** d. **Retention period of documents containing Personal Data** e. **Details regarding the Information collected** f. **The period of processing of Personal Data** g. **Personal Data Subject rights**	○ Records a searchable & sortable forensic record of all file access (open, move, modify, delete, rename), email activity, network events (proxy, VPN, DNS), and permissions changes—scalable to billions of events per day ○ Easily comply with privacy regulations by storing PII properly, ensuring data is shared appropriately, and being able to quickly complete data subject access requests (DSARs) ○ Allows for easy compliance with privacy regulations by storing personally identifiable information properly, ensuring data is shared appropriately, and being able to quickly complete data subject access requests ○ Provides accurate search results that can be easily filtered, copied, or exported into an easy format (PDF reports, Excel files or .CSV files) ○ Allows you to find where a subject's data is being processed in the cloud or in unstructured data stores, and can demonstrate that the processing activity has ceased
Data Subject Rights	
(Article 5) Personal data subjects have the right to obtain information regarding the clarity of identity, legal basis, purpose of request and utilization of personal data, and accountability of the party requesting personal data.	○ Varonis Privacy Automation allows organizations to search their M365 and on premise environments for all PII related to the DSAR. Varonis allows organizations to quickly search for, locate, and collect files with specific PII for DSAR. Varonis allows for the copying of DSAR relevant documents and exporting of search results for use in DSAR support. ○ Provides a unified audit trail — Varonis captures, aggregates, normalises, and analyses every data access event for every user on Windows, UNIX/Linux,

	NAS, Exchange, and SharePoint servers, without requiring native operating system auditing
(Article 6) Personal data subjects have the right to obtain information regarding the clarity of identity, legal basis, purpose of request and utilization of personal data, and accountability of the party requesting personal data.	○ Automatically and accurately classify sensitive and regulated data shared and stored across on-prem and cloud data stores with a scalable classification engine
(Article 7) Personal data subjects have the right to obtain information regarding the clarity of identity, legal basis, purpose of request and utilization of personal data, and accountability of the party requesting personal data.	○ Varonis provides accurate search results that can be easily filtered, copied, or exported into an easy format (PDF reports, Excel files or .CSV files)
(Article 8) Personal data subjects have the right to terminate the processing, delete, and/or destroy their personal data in accordance with the provisions of the applicable laws and regulations.	○ Moves, collects, and secures all sensitive files into one single location to easily quarantine or delete the data — allowing for easier compliance with privacy policies ○ Allows you to find where a subject's data is being processed in the cloud or in unstructured data stores, and can demonstrate that the processing activity has ceased
(Article 10) Personal data subjects have the right to terminate the processing, delete, and/or destroy their personal data in accordance with the provisions of the applicable laws and regulations.	○ Allows you to find where a subject's data is being processed in the cloud or in unstructured data stores, and can demonstrate that the processing activity has ceased
(Article 11) Personal data subjects have the right to terminate the processing, delete, and/or destroy their personal data in accordance with the provisions of the applicable laws and regulations.	○ Allows you to find where a subject's data is being processed in the cloud or in unstructured data stores, and can demonstrate that the processing activity has ceased. ○ Moves, collects, and secures all sensitive files into one single location to

	easily quarantine or delete the data — allowing for easier compliance with privacy policies
(Article 13) Personal data subjects have the right to terminate the processing, delete, and/or destroy their personal data in accordance with the provisions of the applicable laws and regulations.	○ Provides accurate search results that can be easily filtered, copied, or exported into an easy format (PDF reports, Excel files or .CSV files)
Data Protection Impact Assessment	
(Article 34) Personal data subjects have the right to terminate the processing, delete, and/or destroy their personal data in accordance with the provisions of the applicable laws and regulations. Processing of Personal Data with high risk potential as referred to in paragraph (1) includes: a. Automated decision-making that has legal consequences or a significant impact on the Personal Data Subject; b. Processing of specific Personal Data; c. Large-scale processing of Personal Data; d. Processing of Personal Data for systematic evaluation, scoring or monitoring activities of Personal Data Subjects; e. Processing of Personal Data for activities matching or merging a group of data; f. The use of new technology in the processing of Personal Data; and/or g. Processing of Personal Data that restricts the exercise of the Personal Data Subject's rights.	○ Varonis offers a complimentary cyber resiliency risk assessment to measure data exposure and stress test your security stack against the latest adversary tactics and tradecraft. Our team of experts will: • Assess your threat detection capabilities against modern adversaries • Classify sensitive data and measure overexposure and non-compliant access • Document detection gaps, Zero Trust posture, and remediation priorities • Prepare and educate your team to handle advanced incidents
Data Security	

(Article 35) Personal data subjects have the right to terminate the processing, delete, and/or destroy their personal data in accordance with the provisions of the applicable laws and regulations. **a)** The preparation and implementation of technical operational measures to protect Personal Data from interference with the processing of Personal Data that is contrary to the provisions of laws and regulations; and **b)** Determination of the security level of Personal Data by taking into account the nature and risks of the Personal Data to be protected in the processing of Personal Data.	○ Analyses your security gaps, prioritizes your biggest risks and demonstrates progress over time with risk dashboards. ○ Continuous data risk assessment dashboards highlight security issues, such as at-risk sensitive data, excessive permissions, Active Directory (AD) vulnerabilities, stale passwords, and remote worker activity. ○ Reduces your blast radius with predefined audit reports that reveal key risk indicators, shadow accounts, user and group changes, policy modifications, AD misconfigurations and vulnerabilities, and more. Run reports on-demand or email them on a schedule ○ Automatically finds, moves, archives, quarantines, or deletes data based on content type, age, access activity, and more ○ Provides a complimentary Varonis Data Risk Assessment to measure data exposure and stress test your security stack against the latest adversary tactics and tradecraft
(Article 36) In conducting the processing of Personal Data, the Personal Data Controller shall maintain the confidentiality of Personal Data.	○ Allows for easy compliance with privacy regulations by storing personally identifiable information properly, ensuring data is shared appropriately, and being able to quickly complete data subject access requests

(Article 37) The Personal Data Controller shall supervise each party involved in the processing of Personal Data under the control of the Personal Data Controller.	○ Provides an automated workflow for data access requests that puts data owners in charge of data access, enabling you to actively maintain least-privilege access
(Article 38) The Personal Data Controller shall supervise each party involved in the processing of Personal Data under the control of the Personal Data Controller.	○ Provides an automated workflow for data access requests that puts data owners in charge of data access, enabling you to actively maintain least-privilege access ○ Schedules automated entitlement reviews to ensure access permissions are current
(Article 39) The Controller of Personal Data shall prevent Personal Data from being accessed unlawfully. a) The prevention as referred to in paragraph (1) is carried out by using a security system for Personal Data that is processed and/or processing Personal Data using electronic systems reliably, safely, and responsibly. b) Prevention as referred to in paragraph (2) shall be carried out in accordance with the provisions of laws and regulations.	○ Analyses your security gaps, prioritizes your biggest risks, and demonstrates progress over time with risk dashboards. Continuous data risk assessment dashboards highlight security issues, such as at-risk sensitive data, excessive permissions, Active Directory (AD) vulnerabilities, stale passwords, and remote-worker activity. ○ Provides an automated workflow for data access requests that puts data owners in charge of data access, enabling you to actively maintain least-privilege access. ○ Schedules automated entitlement reviews to ensure access permissions are current
Responding to requests from Personal Data Subjects	
(Article 40) The Personal Data Controller shall stop the processing of Personal Data in the event that the Personal Data Subject withdraws the consent to the processing of Personal Data.	○ Allows for easy compliance with privacy regulations by storing personally identifiable information properly, ensuring data is shared appropriately, and being able to quickly complete data subject access requests.

(Article 41) The Controller of Personal Data shall be obliged to postpone and restrict the processing of Personal Data either partially or completely by no later than 3 x 24 (three times twenty-four) hours from the time the Controller of Personal Data receives the request for postponement and restriction of processing of Personal Data.

(Article 42) The Controller of Personal Data shall end the processing of Personal Data in the event that:

(Article 43) The Personal Data Controller shall delete Personal Data in the event that:

(Article 44) The Personal Data Controller shall destroy the Personal Data in the event that:

a. Has reached the retention period;
b. The purpose of processing the Personal Data has been achieved; or
c. There is a request from the Personal Data Subject.

(Article 45) The Personal Data Controller shall notify the deletion and/or destruction of Personal Data to the Personal Data Subject.

- Allows you to find where a subject's data is being processed in the cloud or in unstructured data stores, and can demonstrate that the processing activity has ceased.
- Automatically finds, moves, archives, quarantines, or deletes data based on content type, age, access activity, and more.

Breach Notification

(Article 46) In the event of failure of Personal Data Protection, the Personal Data Controller shall be obliged to submit written notification at the latest 3 x 24 (three times twenty-four) hours to Personal Data Subject and institutions.

The written notification as referred to in paragraph (1) shall at least contain:

a. Disclosed Personal Data;
b. When and how Personal Data is disclosed and handling and recovery efforts for the disclosure of Personal Data by the Personal Data Controller.
c. In certain cases, the Personal Data Controller is obliged to

- Provides a unified audit trail — Varonis captures, aggregates, normalizes, and analyses every data access event for every user on Windows, UNIX/Linux, NAS, Exchange, and SharePoint servers without requiring native operating system auditing.
- Provides pre-built and customizable playbooks for efficient incident response and investigation workflows

inform the public about the failure of Personal Data Protection.	
Accountability	
(Article 47) In the event of failure of Personal Data Protection, the Personal Data Controller shall be obliged to submit written notification at the latest 3 x 24 (three times twenty-four) hours to Personal Data Subject and institutions.	○ DPOs find Varonis' high-level risk dashboards and quantified granular reporting invaluable for prioritising risk mitigation and evidencing good operational data privacy controls and processes.
Privacy Rights	
(Article 56) In the event of failure of Personal Data Protection, the Personal Data Controller shall be obliged to submit written notification at the latest 3 x 24 (three times twenty-four) hours to Personal Data Subject and institutions. In conducting the transfer of Personal Data as referred to in paragraph (1), the Personal Data Controller shall ensure that the country of domicile of the Personal Data Controller and/or the Personal Data Processor receiving the transfer of Personal Data has a level of Personal Data Protection equal to or higher than that stipulated in this Law. In the event that the provisions as referred to in paragraph (2) are not fulfilled, the Personal Data Controller shall be obliged to ensure that there is adequate and binding Personal Data Protection. In the event that the provisions as referred to in paragraph (2) and paragraph (3) are not fulfilled, the Controller of Personal Data must obtain the consent of the Personal Data Subject. Further provisions regarding the transfer of Personal Data are regulated in a Government Regulation.	○ Allows for easy compliance with privacy regulations by storing personally identifiable information properly, ensuring data is shared appropriately, and being able to quickly complete data subject access requests. ○ Allows you to find where a subject's data is being processed in the cloud or in unstructured data stores, and can demonstrate that the processing activity has ceased. ○ Automatically finds, moves, archives, quarantines, or deletes data based on content type, age, access activity, and more.

Ready to experience the Varonis difference

Schedule a free data risk assessment.

Varonis can help manage your security risk and help you comply with PDP by identifying where you have sensitive data, reducing that data's blast radius, and monitoring your data for potential threats. To see where you have PDP data across your environment, sign up for a free PDP risk assessment.

Our complimentary assessment ran by security expects will help you find and classify regulated data across on-premises and cloud data stores, measure data exposure, and alert on suspicious access to regulated information.

Contact us

About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data: sensitive files and emails; confidential customer, patient, and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects cyber threats from both internal and external actors by analyzing data, account activity, and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation.

Varonis products address additional important use cases including data protection, data governance, Zero Trust, compliance, data privacy, classification, and threat detection and response. Varonis started operations in 2005 and has customers spanning leading firms in the financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education sectors.