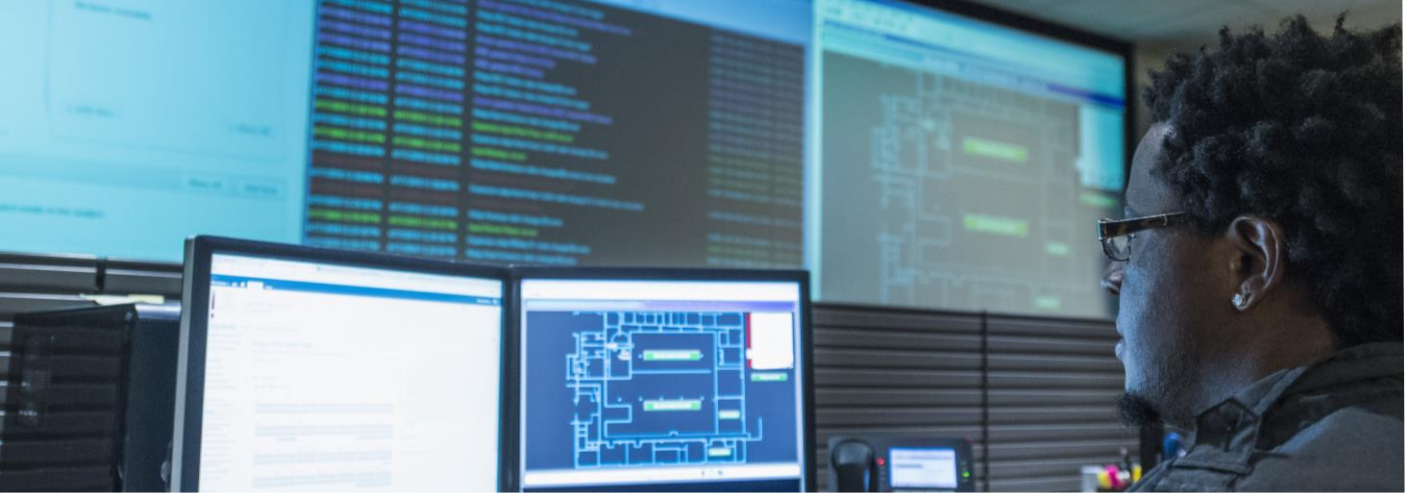

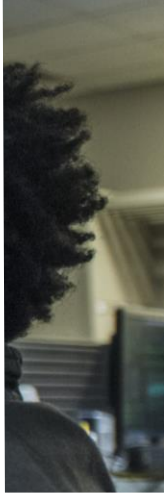

Digital Trust NewsFlash

PwC Digital Services / 2022 年 10 月 / 第 5 号

インドネシア個人情報保護法
P1

インドネシア個人情報保護法

インドネシアの個人情報保護法（PDP）は、2022 年 10 月 17 日にジョコ・ウィドド大統領により批准され、個人情報の保護に関する法律 2022 年第 27 号として掲載されました（以下、「UU PDP」）。

UU PDP は、情報対象者の権利を守るため、個人情報の処理に関するガイドラインと、個人情報の保護に関する情報管理者と情報処理者の義務を規定することを目的としています。また、2019 年法案では定義されていなかった個人情報保護当局（kelembagaan）についても規定されました。

UU PDP の内容

新たな規定と修正点

国会（DPR）は 2019 年 12 月 6 日に PDP 法案を公開し、2022 年 9 月 5 日に修正され、2022 年 9 月 20 日に再公開されました。当初の草案と比較して、2022 年 10 月 17 日に批准された UU PDP の主な相違点・追加規定は以下の通りです。

a. **「同意」**には、子どもや障害者のための規定が含まれている（第 25 条、第 26 条）
b. リスク基準の高い個人情報には、**個人情報保護影響分析（DPIA）**を実施する必要がある（第 34 条）
c. **行政罰**は、年間所得または違反年数に応じた年間売上の最大 2%（第 57 条）

個人情報の保護

UU PDP は、インドネシア国内、またはインドネシア国外で、インドネシアまたはインドネシア国民の個人情報対象者に法的影響を与える行為を行うすべての個人、公共団体、国際機関に適用されます（第 2 条）。

UU PDP におけるいくつかの用語について、以下のように説明されています。

a. **個人情報**とは、直接または間接的に、複合的または単独で、電子的または非電子的に識別される、**識別または識別可能な**個人（自然人・情報主体）に関連する情報。UU PDP では、個人情報を以下の 2 種類に分類している。

1. **一般情報**：氏名、国籍、結婚、性別、宗教など
2. **特定情報**：健康記録、生体情報、遺伝子情報、犯罪記録、子供の情報、財務情報など

b. **個人情報保護当局（Authority/Lembaga）**とは、個人情報保護に関する法律の施行と遵守を監督し、個人情報の権利保護のために設立された国家機関。

c. **情報管理者**とは、情報処理の目的を決定し、情報処理活動に対する管理を実行する際に、個人または共同で行動する個人、公的機関、国際機関。
情報管理者は、以下のことを**実行**しなければならない。
1. 情報処理の合法性、公正性、透明性（第 27 条）
2. 目的に応じた情報処理（第 28 条）
3. 検証による情報の正確性、完全性及び一貫性（第 29 条）

d. **情報処理者**とは、情報管理者に代わって個人情報を個人または共同で処理する個人、公的機関、国際的な組織。

e. **情報保護責任者（DPO）**は、以下の基準のいずれかを満たす組織に義務付けられている(第 53 条)。
1. 公共の利益のために個人情報を処理する。
2. 情報管理者の主な活動に、大規模な個人情報の継続的かつ体系的な監視が含まれる。
3. 情報管理者の主な活動に、特定の個人情報または犯罪情報に関連する個人情報の処理が含まれる。

DPO は、専門性、法律、個人情報保護実務に関する知識、および職務遂行能力に基づき任命されなければなりません。DPO は内部の情報管理者・情報処理者または外部の関係者から任命することができます。最低限の DPO の義務は、以下の通りです(第 54 条)。
1. UU PDP の遵守について、情報管理者・情報処理者に通知し、助言する。
2. UU PDP 及び情報管理者・情報処理者のポリシーの遵守状況を監視し、確認する。
3. DPIA への助言および情報管理者・情報処理者のパフォーマンスを監視する。
4. 情報処理に関連する問題の調整し、連絡役となる。

f. **情報主体または個人**とは、個人情報に関連する人物と定義される。UU PDP 第 5 条から第 13 条に定義される情報対象者の権利は以下のとおり：
1. 情報提供を受ける権利
2. 修正する権利
3. アクセスする権利
4. 消去する権利
5. 情報処理を制限する権利
6. 自動化された意思決定およびプロファイリングに関連する権利
7. 異議を申し立てる権利
8. 補償を請求する権利
9. データポータビリティの権利

個人情報の処理

個人情報の処理には、個人情報の収集、保存、処理、転送、更新、および破棄が含まれます。第 20 条によると、個人情報の処理には以下のような法的根拠が必要とされています。

a. 電子的または非電子的な文書の形式による情報対象者の明示的な同意が必要であり、これには個人情報の処理要求からなる同意条項が含まれる。
1. **子供の情報処理**には、**親権者**または**保護者**の同意が必要(第 25 条)。
2. **障害のある人の情報**処理には、**情報主体**または**保護者**の同意が必要(第 26 条)。

b. 契約の履行

c. 正当な利益

d. 重要な利益
e. 法的要求事項
f. 公共の利益

また、個人情報を処理する際には、以下のような個人情報保護の原則を遵守しなければなりません。

a. 適法性、公正性、透明性
b. 目的の制限
c. データの最小化
d. 正確性
e. 保存の制限
f. 完全性・機密性
g. 説明責任

個人情報を処理している間、情報管理者はすべての個人情報処理活動の記録（ROPA）を保持する義務があります（第 31 条）

情報侵害

情報侵害が発生した場合、3×24 時間以内に、関連する情報対象者および当局に書面で報告する必要があります。ただし、場合によっては、情報管理者は、情報侵害について公表する義務もあります。書面による通知には、少なくとも以下の詳細が含まれていなければなりません。

a. どのような個人情報が侵害されたのか。
b. 情報侵害がいつ発生したか。
c. どのように情報侵害が発生したか。
d. どのような是正措置が取られたか（第 46 条）

情報管理者の義務

UU PDP 第 21 条によると、情報管理者は情報対象者の同意を得るにあたり、情報処理の合法性、情報処理の目的、処理される個人情報の種類と関連性、保存期間、収集した情報、情報処理の期間、情報対象者の権利についてプライバシー通知しなければなりません（プライバシーポリシー）。プライバシー通知に変更がある場合、情報管理者は事前に情報対象者に告知しなければなりません。

a. 情報管理者は、情報対象者からの要求を受けてから **3 x 24** 時間以内に以下の作業を**完了**しなければならない。
    1. 情報対象者の要求に従って個人情報を修正すること（第 30 条）
    2. 処理された個人情報およびその履歴記録へのアクセスを許可すること（第 32 条）
    3. 情報処理活動を停止すること（第 40 条）
    4. 情報処理活動を延期および制限すること（第 41 条）
b. 情報管理者は、以下の場合に情報処理活動を**停止**しなければならない。
    1. 保存期間に達した場合。
    2. 情報処理の目的が達成された場合
    3. 情報対象者が情報処理に異議を申し立てた場合（第 42 条）
c. 情報管理者は、以下の場合に個人情報を**消去**しなければならない。
    1. 個人情報が処理目的ために必要でなくなった場合。
    2. 情報対象者が同意を撤回した場合
    3. 情報対象者が情報処理に異議を申し立てた場合
    4. 個人情報が違法に収集・処理された場合（第 43 条）

d. 情報管理者は、以下の場合に個人情報を**破棄**しなければならない。
    1. 保存期間が終了し、廃棄が必要となった場合
    2. 情報対象者が情報処理に異議を申し立てた場合
    3. 個人情報が紛争解決過程に関係していない場合
    4. 個人情報が違法に収集された場合（第 44 条）

情報管理者の義務の免除は、国家防衛と安全保障、法の執行、公共の利益、国家管理を目的とする金融サービス当局の利益に適用されます(第 50 条)。

個人情報の移転

個人情報の移転は、以下の条件のもとに許可されます。

a. UU PDP に規定されたインドネシアの法定領土**内**(第 55 条)。
b. インドネシアの法定領土**外**では、以下の規定が適用される(第 56 条)。
    1. 情報を受け取る情報管理者または情報処理者の居住国が、UU PDP と同等またはそれ以上の個人情報保護レベルを有していることを確認すること
    2. 適切な個人情報保護があり、その保護に拘束力があることを確認すること
    3. 情報転送に関する個人情報対象者の同意が得られていること

高リスクの基準

情報管理者は、個人情報処理活動において個人情報保護の原則を遵守しなければならず、情報対象者に対する**リスクを高める可能性がある場合、情報管理者は DPIA を実施することが義務付けられています**。高リスクの基準は以下の通りです (第 34 条):

a. 自動化されている意思決定
b. 特定の情報処理
c. 大規模な情報処理
d. 体系的なモニタリング
e. 情報照合
f. 革新的な技術
g. サービスの拒否

考慮すべき点

UU PDP に準拠するためには、少なくとも以下の作業を行う必要があります。

No	分野	定義	該当規制
1	**プライバシーガバナンス**	• プライバシー戦略の策定 • プライバシーに関するガバナンス体制(DPO 事務局など)の策定 • 情報保護責任者(DPO)の選任	• 情報管理者と情報処理者の義務に関する UU PDP 第 VI 章 • DPO に関する UU PDP 第 53 条～第 54 条
2	**ポリシーマネジメント**	• プライバシーポリシーの策定 • 情報保護影響評価(DPIA)	• 情報対象者の権利に関する UU PDP 第 IV 章 • 個人情報処理に関する UU PDP 第 5 章 • DPIA に関する UU PDP 第 34 条
3	**クロスボーダーデータ戦略**	• クロスボーダーデータプライバシープロセスの確立	• 国境を越えるデータ移転に関する UU PDP 第 VII 章
4	**データライフサイクルマネジメント**	• データライフサイクル文書の確立 • 情報処理活動記録(ROPA) • 情報保持ポリシーの更新	• 個人情報処理に関する UU PDP 第 V 章 • 情報管理者の義務に関する UU PDP 第 VI 章第 2 部 • ROPA に関する UU PDP 第 31 条 • 情報の保持と消去に関する UU PDP 第 42 条～第 45 条
5	**情報対象者の権利**	• 情報対象者の権利プロセスの確立 • 同意管理プロセスの確立 • 同意管理ツールの導入(該当する場合)	• 情報対象者の権利に関する UU PDP 第 IV 章

No	分野	定義	該当規制
6	**情報セキュリティ**	• 情報保護プログラムの策定 • 第三者リスクアセスメントの強化 • 情報セキュリティポリシーの更新 • 情報保護ツールの導入	• 情報セキュリティに関する UU PDP 第 35 条～第 37 条、第 39 条
7	**インシデント管理**	• インシデント対応と情報侵害の対応力の強化	• 情報侵害の報告に関する UU PDP 第 46 条
8	**情報処理者の信頼性**	• 第三者管理の改善 • 第三者との契約更新	• 情報処理者の義務に関する UU PDP 第 VI 章第 3 部
9	**トレーニングおよび意識向上**	• 個人情報・プライバシーに関するトレーニングおよび意識の向上	• 意識向上および社会化に関する UU PDP 第 63 条

個人情報を収集し、処理する目的を理解することは、組織にとって最も重要なものです。個人情報保護法の遵守は、法務部門やコンプライアンス部門だけに任せておくことはできません。UU PDP を遵守するためには、組織の全員が個人情報を保護する責任を理解する必要があります。インドネシア市民の個人情報を処理（収集、保存、転送を含む）するすべての企業および国外の機関は UU PDP に準拠する必要があります。

移行期間

情報管理者、情報処理者、および個人情報処理活動に関連するその他の関係者は、**法律の批准から最大 2 年以内に** UU PDP を遵守しなければならず、個人情報の保護に関するすべての法令の規定は、UU PDP の規定に抵触しない限り、有効とみなされます。

罰則規定

本規定に違反した場合、書面による警告、**個人は 60 億ルピア、法人は 600 億ルピアの刑事罰則、年間所得または違反年数に応じた年間売上の最大 2%の行政罰、6 年以下の懲役、**活動の一時停止、法人の解散などの罰則が科される場合があります。

Your PwC Indonesia Contacts:

Subianto
Broader Assurance Services Leader
Chief Digital & Technology Officer
subianto.subianto@pwc.com

Indra Allen
Legal Partner
indra.allen@pwc.com

Andrew Tirtadjaja
Cybersecurity & Privacy Director
andrew.tirtadjaja@pwc.com

Jeffry Kusnadi
Cybersecurity & Forensics Director
jeffry.kusnadi@pwc.com

Beatrix Ariane
Cybersecurity & Privacy Senior Manager
beatrix.b.ariane@pwc.com

Roro Astuti
Legal Senior Manager
roro.astuti@pwc.com

Ricky Riswanto
Cybersecurity & Forensics Senior Manager
ricky.riswanto@pwc.com

Yusri Amsal
Cybersecurity & Forensics Senior Manager
yusri.amsal@pwc.com

www.pwc.com/id

PwC Indonesia

@PwC_Indonesia

pwc