ADP Counsellors at Law

THE BEST LEGAL SERVICE TO NAVIGATE YOUR BUSINESS

Insight

Data Confidentiality in Financial Sector Professional Engagements: Shared but Differentiated Responsibility

Bellina Christy S.H., Raditya Gerardi Simarmata.

ADP Counsellors at Law

Plaza Simatupang 6th Floor Kav. IS No. 01, Jl. T.B. Simatupang, RT.2/RW.17, Pd. Pinang, Kec. Kby. Lama, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12310 | info@adplaws.com

Introduction

Supporting professions in the financial services sector, including public accountants, actuarial consultants, public appraisers, notaries, legal consultants, and other professions designated by the Financial Services Authority (OJK), routinely receive information unavailable to the public. Audits, valuations, legal due diligence, actuarial reviews, corporate actions, and regulatory investigations may expose them to customer identities, transaction histories, financial statements, beneficial-ownership records, legal disputes, internal controls, and business strategies.

Once information is delivered to an external professional, institutions sometimes treat the confidentiality risk as having been transferred. That view is incomplete. The service recipient selects the professional, defines the engagement, determines which records are disclosed, controls the initial transfer, and ordinarily decides how the professional's findings will be used. POJK No. 5 of 2025 concerning Supporting Professions in the Financial Services Sector (POJK 5/2025) and Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) therefore operate together. The former establishes sectoral-specific confidentiality obligations; the latter governs the processing lifecycle and allocates duties according to the parties' actual roles.

Confidentiality under POJK 5/2025

Article 17 of POJK 5/2025 requires supporting professionals to remain independent, objective, and professional, maintain the confidentiality of data and information obtained in providing services, and apply professional standards, quality-control standards, and codes of ethics. The phrase data and information is broader than personal data. It may cover corporate records, valuation models, actuarial assumptions, legal opinions, trade secrets, internal investigations, and other information that does not identify an individual but remains confidential in the professional relationship.

The obligation is legally enforceable. Breach of confidentiality or failure to implement professional and quality-control standards may result in suspension of registration for up to one year and an administrative fine of up to IDR 5 billion. Repeated suspension may lead to cancellation of registration. Confidentiality is therefore not merely an ethical promise; it affects the professional's legal capacity to continue operating in the financial sector.

POJK 5/2025 also creates lawful disclosure duties. Supporting professionals must provide information to OJK, comply with summonses, undergo examinations, and submit incidental reports concerning regulatory violations or conditions that may endanger the recipient or its stakeholders. These duties qualify as ordinary confidentiality, but they do not authorize indiscriminate disclosure. Information should remain limited to what is required by law or a valid OJK request, transmitted securely, and documented.

Administrative Sanctions under POJK 5/2025

The confidentiality obligation is legally enforceable. A breach of confidentiality or failure to apply professional and quality control standards may expose a supporting professional to suspension of registration for up to one year and an administrative fine of up to IDR 5 billion. Repeated suspension may lead to cancellation of registration. The consequences are therefore not limited to reputational harm or professional discipline; they may directly affect the professional's legal capacity to continue providing services in the financial services sector.

Administrative sanctions also reinforce the need for institutional oversight. Although POJK 5/2025 imposes the direct confidentiality duty on the supporting professional, a service recipient should not assume that the professional's exposure to sanctions eliminates the recipient's own responsibilities under the PDP Law, contractual commitments, or sector-specific governance requirements. The regulatory regimes operate cumulatively according to the conduct and legal role of each party.

Allocation of Roles under the PDP Law

The PDP Law distinguishes between a Personal Data Controller, which determines the purposes and means of processing, and a Personal Data Processor, which processes data on behalf of a controller. These roles depend on the parties'actual functions rather than contractual labels.

In most professional engagements, the service recipient will act as the controller because it determines the purpose of the engagement, the categories of personal data to be disclosed, and how the professional's work product will be used. It must therefore ensure that the disclosure has an appropriate lawful basis under Article 20 of the PDP Law.

A supporting professional will generally act as a processor, handling personal data solely in accordance with the recipient's documented instructions. However, where professional standards or statutory obligations require the professional to independently determine how certain personal data is reviewed, retained, or disclosed, it may instead act as an independent controller. In some engagements, both parties may also qualify as joint controllers where they jointly determine the purposes and means of processing.

Article 51 of the PDP Laws provides the clearest statutory basis for differentiated responsibility. Processing performed by a processor based on the controller's instruction remains within the controller's responsibility. If the processor acts outside the controller's instructions and purposes, responsibility shifts to the processor for that processing. Where two or more parties jointly determine interconnected purposes and means, Article 18 of the PDP Laws may also treat them as joint controllers and requires an agreement allocating their roles, responsibilities, and relationship, together with a jointly designated contact point.

Duties of the Service Recipient

The recipient cannot use a confidentiality clause as a complete transfer of legal risk. Before disclosure, it should test whether each category of information is necessary, relevant, and consistent with the professional purpose. Transferring an entire customer database when a limited sample would suffice may violate the requirements that processing be limited, specific, lawful, transparent, and aligned with its purpose.

The recipient should conduct due diligence on the professional's governance and security arrangements, including access controls, encryption, storage locations, remote-working practices, subcontractors, confidentiality commitments, incident-response capacity, and return or destruction procedures. It should maintain an inventory of disclosed data, the legal basis relied upon, authorized recipients, and retention periods. Where data-subject rights apply, the recipient should ensure that the professional can help locate records, correct inaccuracies, restrict access, and delete or return data when legally required.

High-risk processing also requires attention. Article 34 may require a data-protection impact assessment where the engagement involves specific personal data, large datasets, systematic monitoring, data matching, automated assessment, or new technology. Although the recipient normally leads the assessment, the professional must provide accurate information about its systems, personnel, methods, subcontractors, and safeguards.

Duties of the Supporting Professional

The supporting professional must use information only for the agreed and lawful professional purpose. Internal access should be restricted on a need-to-know basis, client files should be logically or physically separated, transmissions should use secure channels, and processing activities should be documented. Employees, experts, translators, consultants, and technology providers with access should be subject to equivalent confidentiality and security obligations.

Professional independence does not remove data-protection responsibility. Where a lawyer, notary, appraiser, actuary, or accountant independently determines which records must be examined or retained, the professional should identify the lawful basis and purpose for that independent processing. Records retained for professional accountability should not automatically be repurposed for training, marketing, benchmarking, or unrelated commercial analysis. Any secondary use requires a separate lawful basis and must remain compatible with the rights of data subjects and the confidentiality owed to the client.

Contractual Allocation of Responsibilities

The engagement agreement should translate statutory responsibilities into clear operational obligations. It should identify the parties' roles for each processing activity, define the permitted purposes, data categories, and documented instructions, regulate access and the appointment of subcontractors, and establish security, retention, return, and destruction requirements. It should also require assistance with data-subject requests, regulatory inquiries, audits, and incident investigations, and should specify a professional's internal breach reporting deadline that is materially shorter than the controller's statutory notification period.

Contractual allocation does not replace statutory allocation. The parties may distribute operational tasks, audit rights, indemnities, limitations of liability, and financial consequences between themselves, but cannot contract out of obligations imposed directly by POJK 5/2025 or the PDP Law. A clause describing the professional as a processor will not be determinative where its actual conduct shows that it independently determines the purposes or essential means of a particular processing activity. Likewise, an indemnity may allocate losses internally, but does not prevent OJK, data subjects, or other competent authorities from pursuing the party legally responsible for the relevant violation.

Breach Response and Liability

Article 46 of the PDP Law requires a controller to provide written notification to affected data subjects and the competent institution no later than 3 x 24 hours after a personal-data protection failure. The notification must describe the affected data, when and how the exposure occurred, and the response and recovery measures. The engagement agreement should therefore require the professional to report a suspected incident to the recipient within a materially shorter internal period, preserve evidence, contain the breach, and support the recipient's assessment and notification duties.

Shared responsibility does not mean equal responsibility. Liability depends on who determined the relevant purpose, selected the data, controlled access, chose the system, acted outside documented instructions, or failed to implement safeguards. The recipient may be responsible for excessive or unlawful disclosure or for selecting a provider without adequate controls. The professional may be responsible for unauthorized use, insecure storage, failure to supervise personnel, or processing beyond lawful instructions. Both may be responsible where they jointly designed the processing and jointly failed to control its risks.

Conclusion

POJK 5/2025 and the PDP Law create an integrated confidentiality framework for financial professional engagements. POJK 5/2025 places a direct, sanction-backed duty on supporting professions to protect all confidential data and information obtained in providing services. The PDP Law extends the analysis across the processing lifecycle and allocates obligations according to the parties' actual functions as controllers, processors, or joint controllers.

The correct legal model is shared but differentiated responsibility. The service recipient must ensure that disclosure is lawful, necessary, proportionate, and secure, and must continue to oversee processing after transfer. The supporting professional must maintain professional confidentiality obligations, restrict use to lawful purposes, maintain adequate security, cooperate in the exercise of data-subject rights, and accept responsibility for processing outside lawful instructions.

ADP Counsellors at Law

Office
Plaza Simatupang 6th Floor Kav. IS No. 01, Jl. T.B. Simatupang, RT.2/RW.17, Pd. Pinang, Kec. Kby. Lama, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12310

Email
info@adplaws.com

Tel.
+6221 2270 2291