Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

July-2025. Vol 3. No. 2.
e-ISSN: 2442-7667
pp 739-749

Implementasi Pelindungan Data Pribadi Berupa Nomor Induk Kependudukan (NIK) dan Nomor Pokok Wajib Pajak (NPWP) pada Sistem Pemerintahan Berbasis Elektronik Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Deva Sinta Rahmawati[1], Sinta Dewi Rosadi[2], Amelia Cahyadini[3]
Fakultas Hukum Universitas Padjadjaran
E-mail: deva21002@mail.unpad.ac.id

Abstrak: Pelindungan data pribadi terhadap integrasi data antar instansi pemerintah menjadi langkah strategis guna meningkatkan efisiensi layanan publik yang kolaboratif, aman, dan akuntabel. Penelitian ini membahas implementasi pelindungan data pribadi dalam konteks integrasi data dengan mengacu pada prinsip-prinsip yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, meliputi kewajiban hukum pengendali data, optimalisasi lembaga pengawas, serta mekanisme keamanan dan penanganan terhadap insiden kebocoran data terhadap data yang terintegrasi berdasarkan konsep *Whole of Government.* Namun, proses ini menimbulkan tantangan serius dalam pelindungan data pribadi karena belum adanya mekanisme tata kelola yang kuat serta harmonisasi regulasi terhadap keamanan informasi yang bersifat lintas instansi. Hal tersebut menjadi urgensi bagi pemerintah untuk segera merumuskan regulasi yang memuat mekanisme tata kelola keamanan informasi, pengawasan serta penanganan terhadap data terintegrasi antar instansi dan penguatan lembaga pengawas independen guna menegakkan standar pelindungan data serta mengkoordinasikan keamanan informasi, sesuai dengan amanat UU PDP. Dalam penelitian ini, penulis menggunakan metode yuridis normatif dengan pendekatan deskriptif analitis, serta pengumpulan data melalui studi kepustakaan dengan mengkaji Peraturan Perundang-Undangan yang berlaku serta Standar Operasional keamanan informasi dari instansi terkait, dan wawancara semi-terstruktur.

Abstract: *Personal data protection for data integration between government agencies is a strategic step to increase the efficiency of collaborative, safe, and accountable public services. This study discusses the implementation of personal data protection in the context of data integration by referring to the principles stipulated in Law Number 27 of 2022 concerning Personal Data Protection, including the legal obligations of data controllers, optimization of supervisory institutions, and security mechanisms and handling of data leak incidents against integrated data based on the Whole of Government concept. However, this process poses serious challenges in protecting personal data due to the absence of a strong governance mechanism and harmonization of regulations on cross-agency information security. This is an urgency for the government to immediately formulate regulations containing information security governance mechanisms, supervision and handling of integrated data between agencies and strengthening independent supervisory institutions to enforce data protection standards and coordinate information security, in accordance with the mandate of the PDP Law. In this study, the author uses a normative legal method with a descriptive analytical approach, as well as data collection through literature*

Article History
Received: June 15, 2025
Revised: June 22, 2025
Published: July 10, 2025

Kata Kunci:
Pelindungan Data Pribadi, Integrasi Data, Pelayanan Publik, *Whole of Government.*

Keywords :
Personal Data Protection, Data Integration, Public Services, Whole of Government.

Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

July-2025. Vol 3. No. 2.
e-ISSN: 2442-7667
pp 739-749

studies by reviewing applicable laws and regulations and information security Standard Operating Procedures from related agencies, and semi-structured interviews.

https://doi.org/10.5281/zenodo.15857274
This is an open-access article under the CC-BY-SA License.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital di berbagai sektor, termasuk dalam tata kelola pemerintahan, khususnya pelayanan publik. Ketika berbicara mengenai tata kelola pemerintahan berbasis elektronik, maka hal tersebut erat kaitannya dengan Sistem Pemerintahan Berbasis Elektronik (SPBE) atau *electronic government (e-government).* Penerapan SPBE sebagai *e-government* merupakan cerminan dari legitimasi serta hubungannya dengan masyarakat. Selain itu, *e-government* menciptakan hubungan langsung antara masyarakat dengan penyedia layanan publik, dalam hal ini adalah pemerintah.[1] Salah satu bentuk transformasi tersebut adalah dengan adanya integrasi data yang bersifat lintas instansi berupa pemadanan Nomor Induk Kependudukan (NIK) sebagai Nomor Pokok Wajib Pajak (NPWP) bagi Wajib Pajak orang pribadi yang diperkenalkan oleh Direktorat Jenderal Pajak (DJP) pada awal 2023. Kebijakan ini disebut dengan *Single Identity Number* (SIN) yang memuat berbagai informasi mengenai data diri, data finansial, informasi kepemilikan aset, dan lainnya yang bertujuan untuk mengurangi penggunaan kartu identitas.[2]

Pelaksanaan kebijakan ini didukung oleh adanya perjanjian kerja sama antara Direktorat Jenderal Pajak (DJP) dan Direktorat Jenderal Kependudukan dan Catatan Sipil (Ditjen Dukcapil) mencakup pemanfaatan Nomor Induk Kependudukan (NIK), data kependudukan, dan Kartu Tanda Penduduk Elektronik (e-KTP) dalam layanan Direktorat Jenderal Pajak sebagai bagian dari upaya integrasi data untuk mendukung penggunaan NIK sebagai NPWP.[3] Perjanjian ini merupakan kelanjutan mengenai kemitraan antara DJP dengan Ditjen Dukcapil yang telah dimulai sejak tahun 2013 serta adendum kerja sama yang sebelumnnya telah ditandatangani pada 2 November 2018 yang bertujuan memperkuat integrasi data, khususnya terkait dengan penggunaan NIK dan NPWP.

Selain itu, proses pemadanan ini juga guna memenuhi amanat Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan, yang mengatur penggunaan Nomor Induk Kependudukan (NIK) sebagai Nomor Pokok Wajib Pajak (NPWP) bagi wajib pajak orang pribadi yang merupakan penduduk Indonesia[4] dan Peraturan Presiden Nomor 83 Tahun 2021, yang mewajibkan pencantuman NIK dan/atau NPWP dalam layanan publik serta mengatur pemadanan dan pemutakhiran data kependudukan dan basis data perpajakan.

Adanya proses integrasi penyatuan antara NIK dan NPWP merupakan salah satu bentuk penerapan konsep *Whole of Government* (WoG). Konsep ini merupakan pendekatan yang menitikberatkan terhadap kolaborasi yang melibatkan kerjasama antar sektor atau lembaga pemerintah *(interagency)* guna menunjang efektivitas terhadap pelayanan publik serta meminimalisir disintegrasi dalam pemerintahan, mewujudkan integrasi kebijakan, program pembangunan dalam pelayanan publik akibat perkembangan teknologi informasi dan dinamika untuk menyatukan institusi pemerintahan sebagai penyelenggara kebijakan dan pelayanan publik.[5] Secara sederhana, WoG lebih

[1] David Brown. (2005). *Electronic Government and Public Administration*, International Review of Administrative Sciences, 71(2).
[2] Even Gio Lumban T. K. (2022). *Modernisasi Administrasi Perpajakan: NIK menjadi NPWP*, Jurnal Pajak Indonesia, 6(2).
[3] Kementerian Keuangan Direktorat Jenderal Pajak. (n.d.). *Integrasi Data Kependudukan dan Data Perpajakan Menuju Implementasi NIK sebagai NPWP Wajib Pajak Orang Pribadi*. Retrieved September 21, 2024, https://pajak.go.id/id/siaran-pers/integrasi-data-kependudukan-dan-data-perpajakan-menuju-implementasi-nik-sebagai-npwp
[4] Ibid.
[5] Munawar Noor. (2020). *Konsep Whole of Government dalam Pelayanan Publik (Antara Harapan dan Realita)*, Jurnal Merah Putih Universitas 17 Agustus 1945 Semarang, 17(1).

July-2025. Vol 3. No. 2.
e-ISSN: 2442-7667
pp 739-749

fokus terhadap kerjasama yang praktis dan efisien yang lebih mudah diakses.[6] Maka penerapan konsep WoG menjadi dasar penting dalam mewujudkan sinkronisasi data antara Ditjen Dukcapil dan Ditjen Pajak terkait dengan pengintegrasian NIK dan NPWP. Dengan adanya proses integrasi ini, diharapkan dapat menjadi langkah guna memperkuat upaya penegakan kepatuhan perpajakan. Dengan data kependudukan yang menjadi sumber utama bagi berbagai instansi, pengawasan terhadap kepatuhan pajak bisa lebih efektif.

Dalam proses integrasi data, DJP dengan Ditjen Dukcapil bertindak sebagai Pengendali Data Pribadi yang memproses Data Pribadi berupa NIK dan diintegrasikan menjadi NPWP. Sebagaimana tertuang dalam Pasal 18 ayat (2) UU PDP menjelaskan bahwa dalam pemrosesan data pribadi yang dilakukan oleh dua atau lebih pengendali data, maka wajib memenuhi syarat minimal, meliputi adanya perjanjian yang mengatur peran dan tanggung jawab, tujuan serta metode pemrosesan bersama, dan penunjukan narahubung yang ditunjuk secara bersama-sama.[7] Setiap data yang diintegrasikan merupakan data pribadi yang dimiliki oleh orang-perorangan, hal tersebut telah tertuang dalam Pasal 1 ayat (1) UU PDP yang memberikan penjelasan bahwa data pribadi didefinisikan sebagai informasi mengenai seseorang yang dapat diidentifikasi secara khusus, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun non-elektronik, baik secara tersendiri maupun dikombinasikan dengan informasi lainnya.[8]

Sebagaimana tertuang dalam Pasal 1 ayat (12) Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan bahwa Nomor Induk Kependudukan (NIK), adalah nomor identitas Penduduk yang bersifat unik atau khas, tunggal dan melekat pada seseorang,[9] serta tercantum dalam setiap dokumen kependudukan, meliputi, NPWP, KTP, Paspor, SIM, *social security number*, atau data layanan kesehatan tentang keadaan fisik seseorang, kondisi kejiwaan dan mental, kondisi ekonomi, atau data kesehatan, *biometric* seperti sidik jari, retina mata maupun wajah seseorang, serta DNA.[10] Oleh sebab itu, NIK dapat diklasifikasi sebagai data pribadi yang bersifat spesifik sebagaimana telah dijelaskan dalam Pasal 4 ayat (2) UU PDP dan harus mendapatkan pelindungan yang lebih tinggi mengingat sifatnya yang sensitif dan potensi risiko yang lebih besar terhadap hak privasi individu apabila terjadi penyalahgunaan.

Sebagai langkah preventif, Undang-Undang Pelindungan Data Pribadi telah mengamanatkan beberapa upaya guna meningkatkan pelindungan data pribadi. Dalam Pasal 31 UU PDP mengamanatkan setiap pengendali data pribadi untuk menerapkan perekaman terhadap seluruh pemrosesan data pribadi[11] atau *Record of Processing Activities* (RoPA) meliputi rekam jejak pemrosesan data pribadi dari pemohon subjek data pribadi.[12] Dokumen rekam jejak tersebut harus diperbarui secara berkala apabila dalam pelaksanaannya terdapat perubahan data. Setelah penyusunan RoPA, Pasal 34 UU PDP mengamanatkan pelaksanaan *Data Protection Impact Assessments* (DPIA) untuk menilai dan mengurangi risiko tinggi dalam pemrosesan data pribadi termasuk dalam pemrosesan data pribadi berisiko tinggi terhadap subjek data pribadi, contohnya dalam melakukan pemrosesan persetujuan otomatis, bersifat spesifik, berskala besar, *profiling* atau pemrosesan data pribadi untuk kegiatan evaluasi, hingga pemantauan yang sistematis terhadap subjek data pribadi serta pencocokan data untuk kegiatan pemrosesan atau penggabungan sekelompok data.[13]

Dalam DPIA, penting untuk menilai berbagai risiko privasi yang mungkin timbul, seperti risiko akses tidak sah terhadap data pribadi oleh pihak yang tidak berwenang, risiko pengungkapan

[6] Tom Christensen. (2007). *The Whole-of-Government Approach to Public Sector Reform*, Public Administration Review, November–December, 1061–1062.
[7] Pasal 18 (2) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
[8] Pasal 1 (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
[9] Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.
[10] Sinta Dewi Rosadi, Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022), Sinar Grafika, Jakarta Timur, 2023, hlm 29
[11] Pasal 31 UU Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
[12] Pasal 88 (3) Rancangan Peraturan Pemerintah tentang Peraturan Pelaksana Undang-Undang PDP.
[13] Heriani, F. N. (2024). Memahami Data Protection Impact Assessments Dalam Perlindungan Data Pribadi. Retrieved November 27, 2024, Memahami Data Protection Impact Assessments Dalam Perlindungan Data Pribadi

July-2025. Vol 3. No. 2.
e-ISSN: 2442-7667
pp 739-749

data pribadi kepada pihak ketiga tanpa izin, risiko pemrosesan data pribadi untuk tujuan yang tidak sesuai dengan yang telah diinformasikan kepada individu, serta risiko kerusakan atau kehilangan data pribadi akibat kesalahan teknis atau bencana alam.[14] Langkah lainnya dalam meningkatkan keamanan informasi terhadap data pribadi dapat berupa penerapan prosedur keamanan berupa akses, audit, otentikasi, otorisasi dan enkripsi dari ancaman dalam *cyberspace*.

Selanjutnya, upaya represif yang dapat dilakukan oleh instansi terkait terhadap pelanggaran pengelolaan data pribadi dalam pemrosesan data pribadi berupa NIK-NPWP dapat merujuk kepada Undang-Undang Pelindungan Data Pribadi, khususnya Pasal 57 berupa sanksi administratif, serta Pasal 67 s.d. 69 UU PDP terkait ketentuan pidana. Hal tersebut merupakan dasar hukum sebagai upaya Dukcapil dan DJP untuk menindak tegas pelanggaran yang terjadi dalam pemrosesan data pribadi termasuk kebocoran data.

Meskipun Indonesia telah memiliki regulasi mengenai pelindungan data pribadi, namun tidak menutup kemungkinan bahwa akan muncul tantangan terhadap hal tersebut, mengingat dengan semakin masifnya isu dugaan kebocoran data yang terjadi di Indonesia. Berdasarkan data yang dikemukakan oleh BSSN, tercatat pada tahun 2023 terdapat 103 dugaan insiden kebocoran data. Lalu pada 18 September 2024, terdapat dugaan adanya kebocoran data berupa NIK dan NPWP kurang lebih sebanyak 6,6 juta data yang disampaikan oleh Konsultan Keamanan Siber, Teguh Aprianto, melalui unggahan pada akun X pribadinya.[15]

Berdasarkan masalah tersebut, artikel ini akan membahas terkait pemenuhan kewajiban hukum yang dilakukan oleh Ditjen Dukcapil serta DJP sebagai pengendali data pribadi terhadap data yang terintegrasi dalam penerapan sistem *Single Identity Number* (SIN) berdasarkan Undang-Undang Pelindungan Data Pribadi serta mekanisme penanganan apabila terjadi dugaan kebocoran data dalam penerapan sistem *Single Identity Number* (SIN) yang dapat dilakukan oleh Ditjen Dukcapil dan DJP berdasarkan konsep *Whole of Government.*

METODE PENELITIAN

Metode yang digunakan penulis dalam penulisan skripsi ini adalah metode penelitian hukum dengan pendekatan yuridis normatif. Pendekatan yuridis normatif merupakan metode penelitian yang berfokus pada penelitian kepustakaan dengan meneliti bahan pustaka berupa data primer maupun sekunder yang kemudian disusun secara sistematis. Pendekatan ini menggunakan regulasi atau perundang-undangan relevan *(statute approach)* yang sesuai dengan permasalahan yang diteliti.

HASIL DAN PEMBAHASAN

Pemenuhan Kewajiban Hukum oleh Direktorat Jenderal Kependudukan dan Pencatatan Sipil dan Direktorat Jenderal Pajak Terkait Pemrosesan Data Pribadi NIK dan NPWP Melalui Integrasi Data Dalam Penerapan Sistem Single Identity Number (SIN) Berdasarkan Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Integrasi data antara Nomor Induk Kependudukan (NIK) dan Nomor Pokok Wajib Pajak (NPWP) merupakan salah satu langkah fundamental yang diambil pemerintah dalam rangka memperkuat sistem administrasi perpajakan nasional serta mendukung terwujudnya kebijakan Satu Data Indonesia. Dalam memproses serta menghimpun data kependudukan, Ditjen Dukcapil memiliki sistem khusus yang disebut Sistem Administrasi Kependudukan (SAK).[16] Selanjutnya, dalam melakukan pelindungan terhadap data pribadi yang dihimpun, terdapat Sistem Manajemen Keamanan Informasi Administrasi Kependudukan (Selanjutnya disebut SMKI), yaitu bagian dari sistem

[14] Oktavia. (2024). *3 Persyaratan Utama ISO 27701*. Retrieved November 28, 2024, from https://osikonsultan.com/3-persyaratan-utama-iso-27701
[15] Riyandanu, M. F. (2024). *6 Juta Data NPWP Diduga Bocor, Jokowi Minta Kominfo dan Kemenkeu Mitigasi*. Retrieved September 21, 2024, from https://katadata.co.id/berita/nasional/66ec0a84e91a3/6-juta-data-npwp-diduga-bocor-jokowi-minta-kominfo-dan-kemenkeu-mitigasi
[16] Pasal 1 (2) Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan.

July-2025. Vol 3. No. 2.
e-ISSN: 2442-7667
pp 739-749

manajemen secara keseluruhan, berdasarkan pendekatan risiko bisnis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan, dan memelihara keamanan informasi terkait pelaksanaan SAK.[17]

Guna mengoptimalkan keamanan informasi di lingkungan Dukcapil, Dirjen Dukcapil membentuk Satuan Tugas Keamanan Informasi (Satgas Keamanan Informasi) yang bertujuan untuk menjalankan fungsi serta tata kelola keamanan aset informasi dalam kegiatan administrasi kependudukan (Adminduk).[18] Adanya SMKI ini bertujuan guna melindungi, menjamin kerahasiaan, keutuhan, dan ketersediaan Aset Informasi SAK dalam bentuk : a. data dan/atau dokumen; b. perangkat lunak; c. aset berwujud; dan d. aset tidak berwujud.[19]

Pengimplementasian SMKI ini sejalan dengan Pasal 40 PP SPBE yang menguraikan dasar hukum kepada pentingnya pengelolaan layanan elektronik yang terintegrasi, efisien, dan berorientasi kepada pengguna untuk menghasilkan tata kelola yang baik dengan melakukan penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) terhadap data, informasi, infrastruktur, dan aplikasi SPBE melalui mekanisme klasifikasi keamanan, pembatasan akses, deteksi modifikasi, penyediaan cadangan dan pemulihan.

Pihak yang memiliki akses langsung terhadap data untuk diproses adalah Unit TIK yang bertugas untuk penyusunan, mendokumentasikan, dan pengkajian ketentuan akses Informasi SAK berdasarkan kebutuhan organisasi dan prasyarat keamanan; pengelolaan akses pengguna; pelaksanaan tanggung jawab pengguna; pengendalian akses jaringan; pengendalian akses ke sistem operasi; pengendalian akses ke aplikasi dan sistem informasi; dan pengendalian perangkat bergerak dan kerja jarak jauh. Dalam hal pengintegrasian NIK dan NPWP, Dukcapil sebagai pengelola atau pengendali data pribadi memberikan hak akses khusus. Hak akses khusus ini merupakan pemberian akses terhadap sistem informasi yang bersifat rahasia dan hanya diberikan kepada pihak yang menandatangani perjanjian kerahasiaan dengan pemakaian terbatas dan dikontrol oleh satuan tugas keamanan informasi. Dalam pengintegrasian ini, DJP dengan Dukcapil telah menandatangani perjanjian kerjasama terkait dengan integrasi pemadanan NIK dan NPWP, maka dari itu, DJP bertindak sebagai pengguna yang dapat mengakses data yang bersifat rahasia sesuai dengan yang tertuang dalam perjanjian kerjasama saja. Sebagaimana tertuang dalam Pasal 23 ayat (3) Permendagri No. 57/2021 bahwa perjanjian tersebut paling sedikit memuat klausul terkait :[20]

1. Perlindungan kepemilikan informasi, rahasia organisasi, dan kekayaan intelektual;
2. Izin menggunakan informasi rahasia;
3. Hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia;
4. Pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan; dan
5. Syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian.

Pengendalian pertukaran informasi, pemantauan sistem, dan pemisahan perangkat dalam SPBE memiliki peran krusial dalam mendukung implementasi integrasi data Nomor Induk Kependudukan (NIK) dan Nomor Pokok Wajib Pajak (NPWP). Pertukaran informasi antara Ditjen Dukcapil dan DJP harus dilakukan melalui mekanisme resmi, dengan penilaian risiko yang memadai serta jaminan keamanan data melalui pengendalian akses, enkripsi, dan penggunaan saluran komunikasi yang aman. Pemantauan sistem melalui audit logging serta pencatatan aktivitas yang memungkinkan deteksi dini terhadap penyalahgunaan data atau akses tidak sah. Selain itu, pemisahan

[17] Pasal 1(10) Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan.
[18] Rahmaniar. (2022). *Kemendagri Siapkan Pedoman Pelaksanaan SMKI.* Rapat Fasilitasi Pelaksanaan Kegiatan Direktorat PIAK, Jakarta. Retrieved May 12, 2025, Kemendagri Siapkan Pedoman Pelaksanaan SMKI .
[19] Pasal 4 Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan.
[20] Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan.

July-2025. Vol 3. No. 2.
e-ISSN: 2442-7667
pp 739-749

lingkungan pengembangan dan operasional memastikan bahwa data sensitif seperti NIK dan NPWP tidak terekspos.

Dengan langkah-langkah ini, integrasi NIK dan NPWP dapat berjalan secara aman, akurat, dan terpercaya sesuai prinsip perlindungan data pribadi yang termaktub dalam Pasal 16 ayat (2) UU PDP. Adanya penilaian risiko terhadap proses pertukaran informasi dalam proses integrasi data ini juga salah satu bentuk implementasi yang diamanatkan oleh UU PDP, khususnya Pasal 34 ayat (1) dimana pengendali data pribadi wajib melakukan penilaian dampak terhadap potensi risiko tinggi atau *Data Protection Impact Assessment* (DPIA). Selanjutnya, dalam meningkatkan sistem keamanan di lingkungan Dukcapil, Unit TIK bertugas untuk menerapkan kriptografi, yaitu sistem keamanan dilakukan dengan cara menyamarkan informasi dan mengubahnya kembali ke informasi awal yang bertujuan untuk melindungi informasi yang tergolong pada informasi rahasia dan terbatas. Selain itu, Dukcapil juga menerapkan enkripsi, autentifikasi, dan pengendalian sambungan jaringan. Proses enkripsi dilakukan dengan 2 (dua) skema, yaitu enkripsi dengan kunci simetris dan enkripsi dengan kunci asimetris. Penerapan dari kunci simetris ini yaitu variabel kunci enkripsi dan dekripsi adalah sama (agar suatu grup dapat berkomunikasi dengan lainnya). Sedangkan enkripsi dengan kunci asimetris yaitu penerapannya menggunakan kunci enkripsi dan pesan/informasi yang terenkripsi dipublikasikan kepada semua orang, namun hanya orang yang memiliki akses kunci dekripsi saja yang dapat membaca pesan/informasi tersebut.[21]

Sebagai upaya dalam melindungi keamanan informasi, selanjutnya Dukcapil juga menerapkan audit internal yang dilakukan secara rutin minimal selama 1 (satu) tahun sekali atau apabila diperlukan sesuai dengan permintaan Direktur Jenderal Dukcapil. Proses audit internal dilakukan oleh Tim Internal Audit dan wajib telah mengikuti pelatihan Internal Auditor SMKI 27001:2013. Audit internal dilakukan terencana dan sebelumnya telah tersosialisasi kepada Auditor, *Auditee,* dan pihak terkait lainnya. Lalu, dalam pencatatan aktivitas pengguna, , pengecualian, dan kejadian keamanan informasi, Ditjen Dukcapil menerapkan *audit logging,* yaitu proses pencatatan dan pemantauan aktivitas yang terjadi dalam sistem, baik dalam sistem operasi, aplikasi, atau infrastruktur lain yang menghasilkan *log audit.* Hal tersebut merupakan salah satu rekaman kronologis dari berbagai aktivitas dalam teknologi informasi meliputi *login* pengguna, perubahan konfigurasi, dan akses data.[22]

Lalu, DJP yang juga berperan sebagai pengendali data pribadi juga memiliki tata kelola dalam melindungi informasi rahasia. Tata kelola tersebut tertuang dalam Peraturan Direktur Jenderal Pajak Nomor PER-41/PJ/2010 Tahun 2010 tentang Kebijakan Pengelolaan Keamanan Informasi Direktorat Jenderal Pajak (Selanjutnya disebut PER-DJP No. PER-41/PJ/2010) bahwa pelindungan keamanan informasi oleh DJP dilakukan oleh *Chief Information Officer* (CIO) DJP yang merupakan Pejabat Eselon II di unit kerja TIK yang ditunjuk oleh Direktur Jenderal Pajak untuk mengkoordinasikan pelaksanaan tata kelola TIK di lingkungan DJP, sementara Tim Keamanan Informasi yang dibentuk oleh Direktur Jenderal Pajak yang memiliki tugas untuk menjaga dan mengawasi penerapan keamanan informasi, yang diketuai oleh Direktur Teknologi Informasi Perpajakan dan terdiri dari Pejabat serta Petugas Keamanan Informasi.[23]

Dalam mengimplementasikan tata kelola keamanan informasi tersebut, Dirjen Pajak membentuk Tim Keamanan Informasi sebagai Satuan Tugas yang diketuai oleh Ketua Tim Keamanan Informasi DJP yang anggotanya berisikan para Pejabat Keamanan Informasi dan Petugas Keamanan Informasi. Ketua Tim Keamanan Informasi ini memiliki tugas dan kewajiban antara lain bertanggung jawab dalam mengidentifikasi dan menetapkan kepemilikan serta pengelolaan seluruh aset informasi DJP, mengoordinasikan kajian dan pengelolaan risiko keamanan informasi yang berkaitan dengan

[21] Direktorat Jenderal Kependudukan dan Pencatatan Sipil. (n.d.). *SOP Enkripsi*. Retrieved May 21, 2025, from https://drive.google.com/file/u/1/d/1Qg9cqSGQXabtdpXaBZcKtDL6ZSb-Wdf9/view
[22] Learn Microsoft. (2024). *Ikhtisar Pencatatan dan Pemantauan Audit*. Retrieved May 21, 2025, from https://learn-microsoft-com.translate.goog/en-us/compliance/assurance/assurance-audit-logging
[23] Peraturan Direktur Jenderal Pajak Nomor PER-41/PJ/2010 Tahun 2010 tentang Kebijakan Pengelolaan Keamanan Informasi Direktorat Jenderal Pajak.

July-2025. Vol 3. No. 2.
e-ISSN: 2442-7667
pp 739-749

indikator kinerja, serta memelihara rencana kelangsungan layanan TIK setidaknya sekali dalam setahun. Selain itu, Ketua Tim juga wajib memastikan pelaksanaan audit internal secara berkala oleh Auditor Pengelolaan Keamanan Informasi untuk menilai kepatuhan terhadap kebijakan, persyaratan, standar, dan prosedur keamanan informasi, minimal satu kali dalam setahun.

Selanjutnya, fiskus atau aparatur yang ada di bawah DJP wajib menjaga kerahasiaan mengenai data dan informasi wajib pajak yang diatur dalam Pasal 34 ayat (1) UU No. 7 Tahun 2021 bahwa setiap pejabat dilarang mengungkapkan kepada pihak manapun informasi terkait dengan wajib pajak dalam rangka pelaksanaan tugas dan wewenangnya.[24] Pengaturan tersebut sejalan dengan Pasal 40 UU ITE yang sebelumnya telah diuraikan pada kerangka pemikiran, bahwa pemerintah sebagai penyelenggara sistem elektronik wajib mencegah penyebaran informasi yang mengandung data pribadi yang bersifat rahasia. Selanjutnya, dalam hal proteksi data dan penanganan di data center sebagaimana diatur dalam Pedoman Pengamanan Perangkat dan Fasilitas Pengolahan Data dan Informasi di lingkungan DJP, segala aktivitas proteksi data, transfer data dari dan ke perangkat serta fasilitas pengolahan data dan informasi DJP menggunakan *removable media,* yaitu media penyimpan data elektronik yang dapat dipindahkan dan tidak terpasang secara permanen pada komputer, yang hanya boleh diakses oleh pegawai DJP. Setiap data atau informasi yang diklasifikasikan sebagai data sangat rahasia atau rahasia yang tersimpan di *removable media* wajib segera dihapus setelah tidak lagi diperlukan. Selain itu, file yang tidak diketahui asal-usulnya dari *removable media* tidak boleh dibuka sebelum dilakukan pemindaian *antivirus.*[25]

Proses integrasi data dalam penerapan sistem *Single Identity Number* ini merupakan langkah yang dilakukan oleh Ditjen Dukcapil dan DJP sebagai pemenuhan kewajiban mereka terhadap Perjanjian Kerja Sama yang dilakukan oleh kedua instansi tersebut dalam rangka pemanfaatan NIK sebagai NPWP dengan berlandaskan Surat Edaran Dirjen Pajak No. SE-49/PJ/2021 tentang Petunjuk Teknis Pelaksanaan Prosedur Persetujuan Bersama sebagai dasar petunjuk teknis pelaksanaan prosedur persetujuan bersama terkait pemadanan dan pemutakhiran data, termasuk validasi dan pengawasan data tersebut. Perjanjian kerja sama terkait pemadanan NIK dengan NPWP ini selanjutnya tertuang dalam Pasal 2 ayat (1) Peraturan Menteri Keuangan Nomor 136 Tahun 2023 tentang Perubahan Atas Peraturan Menteri Keuangan Nomor 112/PMK.03/2022 Tentang Nomor Pokok Wajib Pajak Bagi Wajib Pajak Orang Pribadi, Wajib Pajak Badan, Dan Wajib Pajak Instansi Pemerintah.

Secara regulasi, Ditjen Dukcapil dengan DJP telah memiliki landasan hukum terkait pengelolaan, keamanan informasi termasuk audit internal, pengelolaan risiko, pembatasan akses, kolaborasi antar unit kerja untuk menjaga kerahasiaan data. Namun, belum adanya dasar hukum terkait tata cara integrasi data yang bersifat lintas instansi atau harmonisasi standar keamanan antar instansi terkait, dimana masing-masing instansi menggunakan standar keamanan berbeda, hal tersebut dapat mengakibatkan adanya tumpang tindih kebijakan. Perbedaan standar ini juga dapat menciptakan celah keamanan berupa peretasan apabila enkripsi atau autentikasinya lemah saat proses pemadanan atau integrasi data. Adanya permasalahan tersebut menimbulkan urgensi bagi pemerintah untuk segera membentuk lembaga pengawas yang bertugas mengawasi kepatuhan pengendali data, menangani pengaduan, serta menjatuhkan sanksi administratif kepada instansi yang gagal dalam melindungi data pribadi, khususnya interoperabilitas data, sesuai dengan amanat Pasal 58 UU PDP.

Mekanisme Penanganan Apabila Terjadi Insiden Kebocoran Data Pribadi Dalam *Sistem Single Identity Number* (SIN) yang Dapat Dilakukan Direktorat Jenderal Kependudukan dan Pencatatan Sipil dan Direktorat Jenderal Pajak Berdasarkan Konsep *Whole of Government*

Guna mendorong transformasi digital dan integrasi data melalui Sistem *Single Identity Number* (SIN) potensi risiko kebocoran data menjadi isu strategis yang perlu mendapatkan perhatian serius, khususnya ketika melibatkan lembaga pemerintah seperti Ditjen Dukcapil dan DJP.

[24] Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan.
[25] Direktorat Jenderal Pajak, Kementerian Keuangan. (n.d.). *Pedoman Pengamanan Perangkat dan Fasilitas Pengolahan Data dan Informasi*. Retrieved May 31, 2025, from https://peraturanpajak.com/wp-content/uploads/2020/09/lampiran-se-45-pj-2020.pdf

July-2025. Vol 3. No. 2.
e-ISSN: 2442-7667
pp 739-749

Sebagaimana dijelaskan dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (selanjutnya disebut PP SPBE) mengatur terkait kerangka kerja dalam mendorong sinergi antar instansi pemerintah melalui integrasi layanan dan pertukaran data yang aman, efektif, dan transparan. Hal tersebut selaras dengan prinsip-prinsip utama dari konsep *Whole of Government.*

Secara khusus, dalam Pasal 45 PP SPBE menekankan integrasi layanan SPBE terhadap sistem data antar instansi pemerintah pusat dan daerah yang bertujuan untuk menghilangkan disintegrasi data sehingga memungkinkan adanya pertukaran data yang cepat, akurat, dan aman. Lebih lanjut, PP SPBE juga mengatur terkait standar teknis dan tata kelola sistem pemerintahan berbasis elektronik agar seluruh aplikasi dan data dapat saling berinteroperasi serta mengharuskan penerapan sistem manajemen keamanan informasi yang melindungi data pemerintah dari ancaman kebocoran, penyalahgunaan, dan gangguan siber. Pengelolaan risiko dan audit internal menjadi bagian integral dari tata kelola SPBE untuk memastikan sistem berjalan dengan aman dan andal.[26]

Hal-hal yang diatur dalam PP SPBE selaras dengan pendekatan konsep *Whole of Government* yang menekankan kolaborasi lintas instansi pemerintah yang bertujuan untuk menghapus sekat-sekat birokrasi dan menciptakan sinergi dalam penyelenggaraan pemerintahan yang lebih efektif, efisien, dan responsif terhadap kebutuhan masyarakat. Maka dari itu, pendekatan ini menjadi fondasi dengan menekankan pentingnya koordinasi dan integrasi antar unit kerja pemerintahan agar dapat bergerak secara harmonis serta mendorong kolaborasi antara kementerian, lembaga, dan pemerintah daerah, seperti yang terlihat dalam integrasi data NIK dan NPWP oleh Ditjen Dukcapil dan Ditjen Pajak, guna meningkatkan efisiensi dan akuntabilitas dalam pelayanan publik.

Guna mendukung layanan administrasi kependudukan dan perpajakan terintegrasi dalam SPBE, Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Integrasi Layanan Digital Nasional (Perpres 82/2023) menegaskan pentingnya percepatan transformasi digital melalui penyelenggaraan aplikasi SPBE yang mengutamakan integrasi, interoperabilitas, koordinasi dan kolaborasi lintas instansi. Maka dari itu, pemadanan NIK dan NPWP merupakan salah satu contoh terhadap prinsip tersebut dalam konteks pelayanan publik.

Selanjutnya, dalam merespons dugaan kebocoran data, DJP telah melakukan kerjasama dengan Kominfo, BSSN, serta Kepolisian Republik Indonesia dengan melakukan penyelidikan meliputi forensik digital untuk melacak pelaku kebocoran data dan mengamankan bukti elektronik dalam menangani kebocoran data pribadi tersebut. Dirjen Informasi dan Komunikasi Publik Kominfo, Prabu Revolusi, memberikan pernyataan terkait dugaan tersebut bahwa Kementerian Kominfo sedang menindaklanjuti dan berkoordinasi secara intensif dengan BSSN, DJP serta Kepolisian RI untuk melakukan investigasi serta mitigasi atas dugaan kebocoran data pribadi.[27] Masing-masing instansi menjalankan tugas dan fungsinya dalam koordinasi ini, dimana Kominfo bertindak untuk memimpin koordinasi teknis dan kebijakan terkait sistem dan keamanan data, DJP sebagai pemilik serta pemroses data memberikan data dan informasi yang digunakan untuk keperluan investigasi, dan Polri bertugas untuk menangani pelanggaran tersebut dengan melakukan penyidikan kriminal siber. Proses koordinasi ini memastikan respons terhadap dugaan kebocoran data secara komprehensif dan terarah sesuai dengan prinsip *Whole of Government.*

Kominfo menegaskan bahwa pelaku kebocoran data dapat dijerat sanksi pidana sesuai dengan ketentuan yang termaktub pada Pasal 67 ayat (1) dan (2) UU PDP bahwa setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi orang lain untuk keuntungan diri sendiri atau orang lain dan merugikan subjek data, dipidana penjara maksimal 5 tahun dan/atau denda hingga Rp5 miliar. Sementara itu, orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi orang lain dipidana penjara maksimal 4 tahun dan/atau denda hingga Rp4 miliar.[28]

[26] Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
[27] Imy. (2024). *Kominfo Gandeng BSSN-Polri Investigasi Dugaan Kebocoran Data NPWP*. Retrieved May 22, 2025, from https://www.cnnindonesia.com/teknologi/kominfo-gandeng-bssn-polri-investigasi-dugaan-kebocoran-data-npwp
[28] Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

July-2025. Vol 3. No. 2.
e-ISSN: 2442-7667
pp 739-749

Semakin masifnya penggunaan teknologi, pemerintah mengeluarkan pedoman untuk menjaga keamanan informasi pada *cyber space,* yaitu Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 4 Tahun 2021 mengatur tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) serta Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik. Peraturan ini merupakan implementasi amanat Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE, khususnya Pasal 41 ayat (4) dan Pasal 48 ayat (5), yang mewajibkan BSSN menyusun pedoman dan standar keamanan informasi bagi penyelenggaraan pemerintahan berbasis elektronik. Pedoman ini berisikan manajemen keamanan informasi SPBE, standar teknis keamanan, prosedur keamanan, peran dan implementasi bagi setiap penyelenggara SPBE di Indonesia yang menjadi landasan instansi pemerintah untuk mengelola keamanan data dan sistem secara sistematis, terstandar, dan berkelanjutan.

Namun, jika dikaitkan dengan mekanisme pengawasan yang dilakukan dalam mengawasi jalannya integrasi data lintas instansi, pedoman tersebut belum mengatur secara spesifik terkait mekanisme pengawasan terhadap pelindungan data pribadi dan penanganan insiden kebocoran data dalam praktik integrasi data sistem *Single Identity Number* yang menitikberatkan terhadap koordinasi lintas instansi. Lalu, dalam UU PDP Pasal 58 sampai dengan 60 dan Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2024 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pasal 41 dan 42 hanya membahas secara umum terkait dengan pengawasan ini.

Mengingat data hasil integrasi dapat termasuk ke dalam kategori data yang bersifat spesifik dan harus mendapat pelindungan yang lebih tinggi, serta potensi terhadap keamanan data terbilang lebih riskan karena menimbulkan lebih banyak celah untuk diretas melalui *middleware* yang menghubungkan dua atau lebih sistem yang berbeda, lalu potensi kegagalan yang diakibatkan oleh segmentasi yang kurang tepat dapat memungkinkan adanya pengaksesan tidak sah dan mengakses seluruh jaringan yang terhubung, maka diperlukan adanya regulasi yang mengatur mekanisme penanganan yang memadai dan bukan hanya menjadi tanggung jawab satu instansi saja, melainkan seluruh instansi terkait, karena sejatinya, dalam hal integrasi data bukan semata-mata hanya dalam konteks pelayanan saja, tetapi harus diiringi dengan penanganan risiko yang dilakukan oleh pemerintah sebagai satu-kesatuan yang utuh, baik dalam pemberian pelayanan publik, khususnya integrasi data, serta penanganan potensi risiko kebocoran data yang sejalan dengan konsep *Whole of Government.*

Meskipun saat ini, Indonesia telah memiliki Undang-Undang tentang pelindungan data pribadi, namun regulasi tersebut masih belum secara spesifik mengatur pelindungan terhadap data yang dihasilkan melalui proses integrasi dan sanksi bagi instansi pemerintah yang gagal melindungi data pribadi yang sifatnya lintas instansi, serta sejauh mana peran antar instansi dalam mempertanggungjawabkan insiden kebocoran data tersebut. Maka dari itu, akibat adanya kekosongan hukum tersebut, Indonesia memerlukan regulasi yang didalamnya mengatur mekanisme pengawasan serta mitigasi penanganan insiden kebocoran data bersifat lintas instansi guna meminimalisir ketidakterpaduan tindakan serta pengalihan tanggung jawab tanpa kejelasan peran antar instansi.

KESIMPULAN

Dalam pemenuhan kewajiban hukum yang dilakukan oleh Ditjen Dukcapil dan DJP, kedua instansi tersebut telah memiliki tata kelola keamanan informasi yang cukup memadai, namun, dalam praktik pemrosesan data pribadi yang bersifat lintas instansi, UU PDP belum secara spesifik mengatur terkait tata cara integrasi data yang bersifat lintas instansi guna menghindari tumpang tindih kebijakan karena masing-masing instansi memiliki standar keamanan yang berbeda. Selanjutnya, lembaga pengawas yang diamanatkan dalam Pasal 58 UU PDP belum sepenuhnya beroperasi yang menyebabkan tidak adanya mediator guna menegakkan standar pelindungan data serta mengkoordinasikan keamanan informasi di lingkungan SPBE.

Selajutmya, dalam mekanisme penanganan insiden siber berdasarkan konsep *Whole of Government* belum berjalan efektif. Hal ini dapat terjadi karena belum adanya SOP atau pedoman khusus bersifat lintas instansi yang berisikan pengaturan secara spesifik terkait dengan mekanisme

July-2025. Vol 3. No. 2.
e-ISSN: 2442-7667
pp 739-749

pengawasan serta penanganan yang dilakukan oleh antar-instansi terhadap potensi kegagalan dalam proses pelindungan data pribadi yang terintegrasi sebagai langkah mitigasi insiden siber.

SARAN

Guna menjamin keamanan dalam pelindungan data pribadi yang bersifat lintas instansi, pemerintah dapat melakukan percepatan pembentukan lembaga pengawas independen sesuai dengan amanat Pasal 58 UU PDP yang secara khusus bertugas untuk mengawasi tata kelola dan integrasi data antar-instansi meliputi evaluasi, investigasi, serta pemberian rekomendasi atas pelanggaran pelindungan data pribadi selama proses integrasi sesuai dengan prinsip-prinsip pelindungan data pribadi.

Langkah strategis yang dapat dilakukan yaitu dengan menerbitkan SOP atau pedoman nasional berisikan regulasi yang secara spesifik mengatur serta menjelaskan peran dan kewajiban masing-masing instansi terkait mekanisme pengawasan dan penanganan yang dilakukan terhadap potensi adanya kegagalan pelindungan data pribadi. Dalam SOP atau pedoman tersebut dapat memuat tugas dan kewajiban masing-masing instansi yang terlibat, pembagian tanggung jawab antar-instansi pengirim dengan penerima data serta mekanisme koordinasi yang bersifat lintas instansi dalam merespon dugaan kebocoran data yang timbul dari adanya pemadanan dan integrasi data antar-instansi guna membangun sistem yang kolaboratif, aman, dan akuntabel sesuai dengan konsep *Whole of Government*.

REFERENSI

Buku

Sinta Dewi Rosadi. (2023), Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022), Jakarta Timur, Sinar Grafika.

Dasar Hukum

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan.

Peraturan Direktur Jenderal Pajak Nomor PER-41/PJ/2010 Tahun 2010 tentang Kebijakan Pengelolaan Keamanan Informasi Direktorat Jenderal Pajak.

Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan.

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Rancangan Peraturan Pemerintah tentang Peraturan Pelaksana Undang-Undang PDP.

Jurnal

David Brown. (2005). *Electronic Government and Public Administration*, International Review of Administrative Sciences, 71(2).

Even Gio Lumban T. K. (2022). *Modernisasi Administrasi Perpajakan: NIK menjadi NPWP*, Jurnal Pajak Indonesia, 6(2).

Munawar Noor. (2020). *Konsep Whole of Government dalam Pelayanan Publik (Antara Harapan dan Realita)*, Jurnal Merah Putih Universitas 17 Agustus 1945 Semarang, 17(1).

Tom Christensen. (2007). *The Whole-of-Government Approach to Public Sector Reform*, Public Administration Review, November–December, 1061–1062.

Website

Kementerian Keuangan Direktorat Jenderal Pajak. (n.d.). *Integrasi Data Kependudukan dan Data Perpajakan Menuju Implementasi NIK sebagai NPWP Wajib Pajak Orang Pribadi*. Retrieved

September 21, 2024, https://pajak.go.id/id/siaran-pers/integrasi-data-kependudukan-dan-data-perpajakan-menuju-implementasi-nik-sebagai-npwp

Heriani, F. N. (2024). *Memahami Data Protection Impact Assessments Dalam Perlindungan Data Pribadi*. Retrieved November 27, 2024, Memahami Data Protection Impact Assessments Dalam Perlindungan Data Pribadi

Oktavia. (2024). *3 Persyaratan Utama ISO 27701*. Retrieved November 28, 2024, from https://osikonsultan.com/3-persyaratan-utama-iso-27701

Riyandanu, M. F. (2024). *6 Juta Data NPWP Diduga Bocor, Jokowi Minta Kominfo dan Kemenkeu Mitigasi*. Retrieved September 21, 2024, from https://katadata.co.id/berita/nasional/66ec0a84e91a3/6-juta-data-npwp-diduga-bocor-jokowi-minta-kominfo-dan-kemenkeu-mitigasi

Rahmaniar. (2022). *Kemendagri Siapkan Pedoman Pelaksanaan SMKI*. Rapat Fasilitasi Pelaksanaan Kegiatan Direktorat PIAK, Jakarta. Retrieved May 12, 2025, Kemendagri Siapkan Pedoman Pelaksanaan SMKI

Direktorat Jenderal Kependudukan dan Pencatatan Sipil. (n.d.). *SOP Enkripsi*. Retrieved May 21, 2025, from https://drive.google.com/file/u/1/d/1Qg9cqSGQXabtdpXaBZcKtDL6ZSb-Wdf9/view

Learn Microsoft. (2024). *Ikhtisar Pencatatan dan Pemantauan Audit*. Retrieved May 21, 2025, from https://learn-microsoft-com.translate.goog/en-us/compliance/assurance/assurance-audit-logging

Direktorat Jenderal Pajak, Kementerian Keuangan. (n.d.). *Pedoman Pengamanan Perangkat dan Fasilitas Pengolahan Data dan Informasi*. Retrieved May 31, 2025, from https://peraturanpajak.com/wp-content/uploads/2020/09/lampiran-se-45-pj-2020.pdf

Imy. (2024). *Kominfo Gandeng BSSN-Polri Investigasi Dugaan Kebocoran Data NPWP*. Retrieved May 22, 2025, from https://www.cnnindonesia.com/teknologi/kominfo-gandeng-bssn-polri-investigasi-dugaan-kebocoran-data-npwp