Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm.118-125
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Analisis Privasi Data Pengguna Shopee Berdasarkan Framework ISO 31000:2018

Siti Safira Tawetubun[*1], Satriani[2]
[1,2] Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia
Email: [*1]13020230217@student.umi.ac.id, [2]13020230073@student.umi.ac.id

(Naskah masuk: *11 Juni 2026*, diterima untuk diterbitkan: *31 Juli 2026*)

Abstrak: *Perkembangan e-commerce di Indonesia telah meningkatkan risiko kebocoran dan penyalahgunaan data pribadi pengguna. Penelitian ini penting karena belum ada studi yang secara spesifik menganalisis privasi data Shopee menggunakan kerangka kerja standar internasional. Penelitian ini bertujuan mengidentifikasi, menganalisis, mengevaluasi, dan memberikan rekomendasi perlakuan terhadap risiko privasi data pengguna Shopee menggunakan framework ISO 31000:2018. Metode penelitian menggunakan pendekatan kualitatif dengan studi literatur terhadap kebijakan privasi Shopee, regulasi Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022, jurnal ilmiah terindeks, dan berita online terkait kasus kebocoran data. Hasil penelitian mengidentifikasi 8 risiko utama (R1-R8) yang meliputi kebocoran data, pencurian akun, penyalahgunaan akses karyawan, pelanggaran UU PDP, serangan ransomware, pembobolan sistem pembayaran, kehilangan data akibat server crash, dan penjualan data ke pihak ketiga. Seluruh risiko berada pada level menengah dengan skor antara 5 hingga 12 berdasarkan perhitungan frekuensi dikalikan dampak. Rekomendasi mitigasi mencakup penerapan enkripsi end-to-end, two-factor authentication wajib, pembentukan tim kepatuhan UU PDP, serta implementasi disaster recovery plan. Penelitian ini berkontribusi sebagai studi pertama yang menggabungkan ISO 31000 dengan objek Shopee dan fokus pada privasi data pengguna.*

Kata Kunci *– E-commerce; ISO 31000; Privasi Data; Shopee*

Abstract: *The development of e-commerce in Indonesia has increased the risk of personal data leakage and misuse. This research is important because no study has specifically analyzed Shopee's data privacy using an international standard framework. This study aims to identify, analyze, evaluate, and provide risk treatment recommendations for Shopee user data privacy using the ISO 31000:2018 framework. The research method uses a qualitative approach with literature study of Shopee's privacy policy, PDP Law No. 27 of 2022, indexed scientific journals, and online news related to data breach cases. The results identified 8 main risks (R1-R8) including data leakage, account theft, employee access misuse, PDP law violations, ransomware attacks, payment system breaches, data loss due to server crashes, and sale of data to third parties. All risks are at the medium level with scores between 5 and 12 based on frequency multiplied by impact calculation. Mitigation recommendations include end-to-end encryption, mandatory two-factor authentication, formation of a PDP law compliance team, and disaster recovery plan implementation. This research contributes as the first study to combine ISO 31000 with Shopee as the object and focus on user data privacy.*

Keywords – *Data Privacy; E-commerce ; ISO 31000; Shopee*

1. PENDAHULUAN

Shopee merupakan platform e-commerce terbesar di Asia Tenggara yang didirikan pada tahun 2015. Perusahaan ini memiliki lebih dari 100 juta pengguna aktif bulanan di Asia Tenggara, dengan kontribusi terbesar berasal dari Indonesia. Shopee menyediakan berbagai layanan digital seperti belanja online, ShopeePay, ShopeeFood, ShopeeLive, serta ShopeeMall. Dalam setiap transaksi yang dilakukan, Shopee secara otomatis mengumpulkan data pribadi pengguna seperti nama lengkap, alamat email, nomor telepon, alamat pengiriman, riwayat transaksi, data lokasi, serta data pembayaran seperti kartu kredit atau e-wallet [1]. Pengumpulan data pribadi dalam skala besar membawa konsekuensi terhadap risiko keamanan data. Pada tahun 2020, data sekitar 15 juta akun pengguna Shopee diduga bocor dan diperjualbelikan di forum online [1]. Peningkatan kasus penipuan mengatasnamakan Shopee dengan modus phishing juga menunjukkan lemahnya kesadaran pengguna terhadap keamanan data [2]. Risiko tidak hanya datang dari eksternal tetapi juga dari internal, seperti penyalahgunaan hak akses oleh karyawan [3].

Kebijakan privasi Shopee mengatur bagaimana data pengguna dikumpulkan, digunakan, dan dilindungi [3]. Di Indonesia, perlindungan data pribadi secara resmi diatur dalam Undang-Undang Nomor 27 Tahun 2022

tentang Perlindungan Data Pribadi (UU PDP) [4]. Regulasi ini mewajibkan perusahaan e-commerce untuk melindungi data pengguna dan memberikan sanksi administratif maupun pidana bagi pelanggar. Sanksi yang diberikan sangat berat, berupa denda hingga 2% dari pendapatan tahunan dan pidana penjara maksimal 4 hingga 6 tahun [5]. Privasi data adalah hak individu untuk mengontrol bagaimana data pribadi mereka dikumpulkan, digunakan, dan disimpan oleh pihak lain [6]. Risiko didefinisikan sebagai pengaruh ketidakpastian terhadap pencapaian tujuan organisasi [7]. Manajemen risiko adalah proses sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, menangani, dan memantau risiko secara berkelanjutan [7]. ISO 31000:2018 adalah standar internasional untuk manajemen risiko yang bersifat generik dan dapat diterapkan oleh berbagai organisasi [7]. Pengelolaan data dalam skala besar merupakan tantangan tersendiri di era digital. Yakin [8] menerapkan metode Content Based Image Retrieval (CBIR) pada sistem pencarian gambar digital, yang mengilustrasikan kompleksitas pengelolaan data multimedia. Pendekatan tersebut memberikan wawasan relevan bagi pengelolaan data pribadi pada platform e-commerce. Prinsip-prinsip dalam pengelolaan data digital ini relevan dengan konteks pengelolaan data pribadi pengguna e-commerce.

Berbagai penelitian sebelumnya telah membahas keamanan data Shopee. Terdapat beberapa keterbatasan penelitian yang menganalisis keamanan data pribadi pengguna Shopee dengan pendekatan deskriptif kualitatif, tetapi tidak menggunakan framework manajemen risiko yang baku [1]. Penelitian meninjau sistem keamanan data Shopee secara umum, tanpa melakukan identifikasi dan analisis risiko secara sistematis [2]. Penelitian membahas tanggung jawab hukum Shopee dalam kasus penyalahgunaan data, namun masih terbatas pada aspek yuridis, bukan manajemen risiko operasional [3]. Penelitian membahas perlindungan hukum data konsumen Shopee dari perspektif hukum, tanpa pendekatan manajemen risiko [6]. Mengidentifikasi berbagai tantangan dan perspektif dalam manajemen risiko pribadi serta privasi data di konteks Indonesia [9]. Beberapa penelitian telah menerapkan ISO 31000 pada e-commerce secara umum [10], [11], [12] belum ada penelitian yang secara spesifik menggabungkan framework ISO 31000 dengan objek Shopee dan fokus pada privasi data pengguna. Menganalisis manajemen risiko TI menggunakan COBIT 2019 dan ISO 31000 pada industri Jumputan, yang menunjukkan bahwa pendekatan terintegrasi dapat diterapkan di berbagai sektor industri termasuk e-commerce yang dilakukan oleh Sutabri [13]. Penelitian tentang efektivitas platform e-commerce dalam mendukung bisnis juga telah dilakukan oleh Muhammad [14], namun fokusnya pada aspek bisnis dan pemasaran, bukan pada privasi data pengguna.

Penelitian ini bertujuan mengidentifikasi risiko-risiko privasi data pengguna Shopee, menganalisis tingkat frekuensi dan dampak dari setiap risiko, mengevaluasi level risiko untuk menentukan prioritas penanganan, dan memberikan usulan perlakuan risiko berdasarkan ISO 31000:2018. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan manajemen risiko privasi data pada platform e-commerce, khususnya Shopee, serta menjadi referensi bagi penelitian selanjutnya di bidang keamanan data dan perlindungan privasi pengguna.

2. METODE PENELITIAN

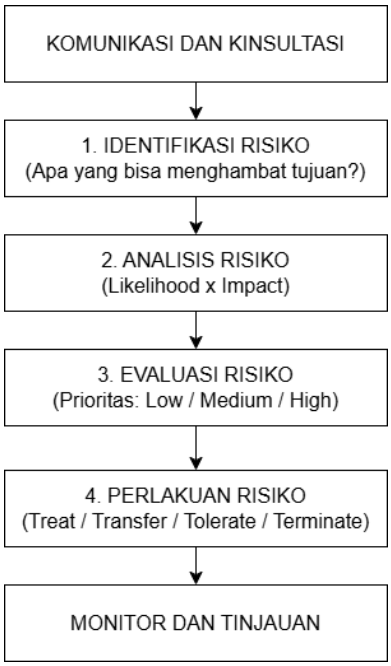
Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur (library research). Metode ini dipilih sejalan dengan tujuan penelitian untuk mengidentifikasi, menganalisis, mengevaluasi, dan memberikan rekomendasi perlakuan risiko privasi data pengguna Shopee berdasarkan kajian terhadap berbagai sumber pustaka yang relevan [7], [10], [11].

2.1. Jenis dan Sumber Data

Penelitian ini menggunakan data sekunder yang diperoleh dari tiga kategori sumber. Pertama, dokumen resmi kebijakan privasi Shopee [4]. Kedua, Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022 [4]. Pendekatan manajemen risiko juga telah dikembangkan oleh National Institute of Standards and Technology (NIST) melalui NIST SP 800-30 yang berfokus pada risiko sistem teknologi informasi [15]. Ketiga, jurnal ilmiah nasional dan internasional terindeks serta media massa berita online terkait kasus kebocoran data Shopee [1], [6], [10].

2.2. Tahapan Penelitian

Penelitian ini mengacu pada siklus manajemen risiko ISO 31000:2018 yang terdiri dari empat tahapan utama, yaitu identifikasi risiko, analisis risiko, evaluasi risiko, dan perlakuan risiko [7], [16]. Gambar 1 menunjukkan tahapan penelitian yang dilakukan.



Gambar 1. Tahapan Penelitian

2.3. Skala Penilaian Risiko

Penilaian frekuensi dan dampak menggunakan skala 1 sampai 5 yang mengacu pada tingkat kemungkinan terjadinya risiko dan tingkat keparahan dampak yang ditimbulkan [10]. Tabel 1 dan Tabel 2 masing-masing menunjukkan skala penilaian frekuensi dan dampak yang digunakan dalam penelitian ini.

Tabel 1. Skala Penilaian Frekuensi

Nilai	Kategori	Keterangan
1	Sangat Kecil	Tidak pernah terjadi > 5 tahun
2	Kecil	Jarang terjadi 3-5 tahun
3	Sedang	Terkadang terjadi 2-4 tahun
4	Berat	Sering terjadi 1-2 tahun
5	Sangat Berat	Pasti terjadi < 1 tahun

Tabel 2. Skala Penilaian Dampak

Nilai	Keterangan
1	Tidak mengganggu aktivitas proses bisnis
2	Sedikit menghambat proses bisnis
3	Mengganggu proses bisnis
4	Menghambat bagian tertentu proses bisnis
5	Menghambat serta mengganggu seluruh proses bisnis

3. HASIL DAN PEMBAHASAN

3.1. Identifikasi Risiko

Berdasarkan kajian terhadap kebijakan privasi Shopee [3], literatur kasus kebocoran data [1], [2], [12], dan regulasi UU PDP [4], ditemukan 8 risiko utama privasi data pengguna Shopee. Tabel 3 menyajikan hasil identifikasi risiko lengkap dengan kode, nama risiko, dan sumber risikonya.

Tabel 3. Identifikasi Risiko Privasi Data Pengguna Shopee

Kode	Kategori	Keterangan

R1	Kebocoran data pribadi pengguna	Peretasan server [1], [2]
R2	Pencurian akun pengguna	Phishing / Social engineering [3]
R3	Penyalahgunaan hak akses karyawan	Human error / Insider threat [17]
R4	Pelanggaran terhadap UU PDP	Ketidakpatuhan regulasi [4], [5], [6]
R5	Serangan ransomware	Malware [11], [18]
R6	Pembobolan sistem pembayaran	Hacker [2]
R7	Kehilangan data akibat server crash	Gangguan teknis [10]
R8	Penjualan data ke pihak ketiga	Kebijakan internal [3], [6]

Berdasarkan Tabel 3, terdapat 8 risiko utama yang dikelompokkan ke dalam lima kategori, yaitu ancaman eksternal (R1, R2, R5, R6), ancaman internal (R3), regulasi (R4), kegagalan sistem (R7), dan kebijakan (R8).

3.2. Analisis Risiko

Analisis risiko dilakukan dengan memberikan nilai frekuensi dan dampak pada setiap risiko yang telah diidentifikasi. Nilai frekuensi dan dampak ditentukan berdasarkan kajian literatur dan kasus-kasus yang pernah terjadi pada platform e-commerce [3], [17]. Tabel 4 menyajikan hasil analisis frekuensi dan dampak untuk kedelapan risiko tersebut.

Tabel 4. Hasil Analisis Frekuensi dan Dampak Risiko Privasi Data Shopee

Kode	Nama Risiko	Frekuensi	Dampak
R1	Kebocoran data pribadi pengguna	2	5
R2	Pencurian akun pengguna	3	4
R3	Penyalahgunaan hak akses karyawan	2	4
R4	Pelanggaran terhadap UU PDP	2	5
R5	Serangan ransomware	2	5
R6	Pembobolan sistem pembayaran	1	5
R7	Kehilangan data akibat server crash	3	4
R8	Penjualan data ke pihak ketiga	1	5

Berdasarkan Tabel 4, nilai frekuensi tertinggi (nilai 3) terdapat pada risiko pencurian akun pengguna (R2) dan kehilangan data akibat server crash (R7). Nilai dampak tertinggi (nilai 5) terdapat pada hampir semua risiko kecuali R2 dan R7 (nilai 4). Hal ini mengindikasikan bahwa sebagian besar risiko privasi data memiliki konsekuensi yang sangat serius terhadap kelangsungan bisnis Shopee.

3.3. Evaluasi Risiko

Evaluasi risiko bertujuan untuk menentukan level prioritas dari setiap risiko berdasarkan kombinasi nilai frekuensi dan dampak. Tingkat risiko ditentukan dengan rumus:

$$Risk\ Score = Frequency \times Impact \quad (1)$$

Kemudian diklasifikasikan ke dalam kategori Rendah (1-4), Menengah (5-12), atau Tinggi (13-25). Tabel 5 menyajikan hasil evaluasi level risiko untuk setiap kode risiko.

Tabel 5. Level Risiko Privasi Data Pengguna Shopee

Kode	Frekuensi	Dampak	Skor Risiko	Level
R1	2	5	10	Menengah
R2	3	4	12	Menengah
R3	2	4	8	Menengah
R4	2	5	10	Menengah
R5	2	5	10	Menengah
R6	1	5	5	Menengah
R7	3	4	12	Menengah

R8	1	5	5	Menengah

Berdasarkan Tabel 5, seluruh risiko privasi data pengguna Shopee berada pada level Menengah dengan nilai tingkat risiko antara 5 hingga 12. Tidak ada risiko yang masuk kategori Tinggi (13-25) maupun Rendah (1-4). Hal ini menunjukkan bahwa semua risiko tersebut memerlukan tindakan pengendalian yang sistematis dan berkelanjutan.

Temuan ini sejalan dengan penelitian yang menganalisis strategi keamanan digital Tokopedia menggunakan ISO 27001 dan ISO 31000, yang juga menemukan bahwa risiko keamanan data pada platform e-commerce umumnya berada pada level menengah [18]. Analisis risiko keamanan informasi menggunakan ISO 31000:2018 dan ISO 27001:2022 menemukan bahwa pendekatan terintegrasi efektif untuk mengidentifikasi dan mengevaluasi risiko di lingkungan digital [16]. Konferensi ACM International Conference menegaskan bahwa analisis risiko TI berbasis ISO 31000 memberikan kerangka kerja yang komprehensif untuk mengidentifikasi dan mengelola risiko keamanan informasi [19].

3.4. Perlakuan Risiko

Perlakuan risiko merupakan tahap akhir dari penilaian risiko yang bertujuan untuk memberikan usulan tindakan dalam menangani setiap risiko yang telah diidentifikasi. Strategi perlakuan risiko yang dapat dipilih meliputi: Accept (menerima risiko), Avoid (menghindari risiko), Transfer (mengalihkan risiko), dan Mitigate (mengurangi risiko) [7], [10], [11]. Tabel 6 menyajikan usulan perlakuan risiko untuk setiap kode risiko.

Tabel 6. Usulan Perlakuan Risiko Privasi Data Shopee

Kode	Level	Usulan Perlakuan Risiko	Rekomendasi
R1	Menengah	Enkripsi end-to-end, penetration testing rutin, update security patch [12], [20]	Mitigate
R2	Menengah	2FA wajib, edukasi phishing, deteksi login mencurigakan [2]	Mitigate
R3	Menengah	Least privilege access, logging akses, pelatihan keamanan [17]	Mitigate
R4	Menengah	Bentuk tim kepatuhan, audit berkala, konsultasi ahli hukum [4], [5]	Mitigate
R5	Menengah	Backup 3-2-1, antivirus, restore drill berkala [11], [18]	Mitigate
R6	Menengah	Tokenisasi, PCI DSS, enkripsi transaksi [2]	Mitigate
R7	Menengah	Disaster Recovery Plan, redundant server, backup harian [10]	Mitigate
R8	Menengah	Kebijakan internal, opsi opt-out, transparansi [3], [6]	Accept

Berdasarkan Tabel 6, terdapat 7 risiko yang direkomendasikan untuk Mitigate (mengurangi risiko melalui penerapan kontrol), dan 1 risiko yaitu penjualan data ke pihak ketiga (R8) direkomendasikan untuk Accept (diterima) dengan catatan Shopee harus transparan dan memberikan opsi kepada pengguna. Literature review mengidentifikasi bahwa strategi keamanan data yang efektif meliputi enkripsi, kontrol akses, dan kepatuhan regulasi [12]. Pentingnya perencanaan manajemen risiko yang terstruktur dalam bisnis e-commerce untuk mengantisipasi berbagai ancaman keamanan data juga telah ditekankan dalam penelitian sebelumnya [20].

3.5. Pembahasan Temuan

Analisis terhadap delapan risiko utama menunjukkan bahwa seluruh risiko berada pada tingkat menengah dengan skor antara 5 hingga 12. Kondisi ini mengindikasikan bahwa meskipun tidak terdapat risiko pada kategori tinggi, seluruh risiko tetap memerlukan pengendalian yang sistematis dan berkelanjutan.

3.5.1. Risiko dengan Dampak Sangat Besar (Skor Dampak 5)

Risiko R1 (kebocoran data pribadi) dengan skor 10 menempati perhatian utama karena dampaknya yang sangat berat (5), meskipun frekuensinya tergolong rendah (2). Kebocoran data umumnya disebabkan oleh celah keamanan server yang dieksploitasi oleh peretas eksternal. Dampak dari kebocoran data sangat luas, meliputi kerugian finansial bagi pengguna, hilangnya kepercayaan publik terhadap platform Shopee, serta

potensi sanksi hukum berdasarkan UU PDP yang dapat berupa denda hingga 2% dari pendapatan tahunan [1], [2], [4].

Risiko R4 (pelanggaran terhadap UU PDP) juga memiliki skor 10 dengan dampak 5. Pelanggaran terhadap regulasi perlindungan data pribadi dapat terjadi akibat ketidakpatuhan Shopee dalam mengelola data pengguna. Sanksi yang diberikan tidak hanya berupa denda administratif tetapi juga pidana penjara bagi pihak yang bertanggung jawab. Oleh karena itu, pembentukan tim kepatuhan khusus dan audit berkala menjadi langkah yang sangat direkomendasikan [4], [5].

Risiko R5 (serangan ransomware) dengan skor 10 juga memiliki dampak sangat berat. Serangan ransomware dapat melumpuhkan seluruh sistem Shopee, mengenkripsi data pengguna, dan meminta tebusan. Selain kerugian finansial, serangan ini dapat mengakibatkan hilangnya data pengguna secara permanen jika cadangan data tidak tersedia. Strategi backup 3-2-1 (3 salinan data, 2 media berbeda, 1 di luar lokasi) dan restore drill berkala menjadi keharusan [11], [18].

Risiko R6 (pembobolan sistem pembayaran) memiliki skor 5 dengan dampak 5. Meskipun frekuensinya sangat kecil (1), konsekuensinya paling serius karena menyangkut data keuangan pengguna seperti nomor kartu kredit dan informasi rekening bank. Implementasi tokenisasi, kepatuhan terhadap standar PCI DSS (Payment Card Industry Data Security Standard), serta enkripsi end-to-end untuk setiap transaksi menjadi strategi mitigasi yang wajib diterapkan [2].

Risiko R8 (penjualan data ke pihak ketiga) juga memiliki skor 5 dengan dampak 5. Risiko ini berkaitan dengan kebijakan internal Shopee yang memungkinkan data pengguna dibagikan kepada mitra bisnis atau pihak ketiga lainnya. Meskipun direkomendasikan untuk di-Accept (diterima), Shopee tetap wajib memberikan transparansi penuh kepada pengguna melalui kebijakan opt-out yang jelas dan mudah diakses [3], [6].

3.5.2. Risiko dengan Frekuensi Tertinggi (Skor Frekuensi 3)

Risiko R2 (pencurian akun pengguna) mencatat skor tertinggi (12) akibat frekuensi yang tergolong sedang (3) dan dampak 4. Teknik phishing dan social engineering menjadi faktor dominan dalam risiko ini. Pencurian akun biasanya terjadi karena pengguna tertipu oleh tautan palsu yang mengatasnamakan Shopee. Penerapan two-factor authentication (2FA) yang wajib bagi seluruh pengguna, edukasi berkala tentang modus phishing, serta sistem deteksi login mencurigakan menjadi strategi mitigasi yang paling efektif [2], [3].

Risiko R7 (kehilangan data akibat server crash) juga memiliki skor 12 dengan frekuensi 3 dan dampak 4. Gangguan teknis pada server dapat disebabkan oleh lonjakan trafik, kesalahan konfigurasi, atau kerusakan hardware. Kehilangan data akibat server crash dapat mengganggu operasional bisnis dan merugikan pengguna yang transaksinya tidak terekam. Implementasi Disaster Recovery Plan (DRP), penggunaan redundant server, serta backup data harian menjadi solusi utama untuk mengantisipasi risiko ini [10].

3.5.3. Risiko Internal

Risiko R3 (penyalahgunaan hak akses karyawan) memiliki skor 8 dengan dampak 4 dan frekuensi 2. Risiko ini bersifat internal dan sering kali tidak terdeteksi karena berasal dari karyawan yang memiliki akses sah ke sistem. Penyalahgunaan akses dapat berupa kebocoran data yang disengaja maupun ketidaksengajaan (human error). Penerapan prinsip least privilege (hak akses seminimal mungkin), logging dan monitoring akses secara berkala, serta pelatihan keamanan rutin bagi karyawan menjadi strategi mitigasi yang direkomendasikan [17].

3.5.4. Implikasi Manajerial

Secara keseluruhan, temuan ini mengindikasikan bahwa meskipun Shopee telah memiliki kebijakan privasi, implementasi teknis dan tata kelola risiko masih memerlukan peningkatan yang sistematis. Shopee perlu memprioritaskan penanganan risiko dengan dampak sangat berat (R1, R4, R5, R6, R8) meskipun frekuensinya rendah, karena konsekuensinya dapat mengancam kelangsungan bisnis. Di sisi lain, risiko dengan frekuensi tinggi (R2 dan R7) memerlukan perhatian pada aspek operasional dan edukasi pengguna.

Rekomendasi utama yang dapat diberikan kepada Shopee meliputi penerapan enkripsi end-to-end untuk seluruh data pengguna, kewajiban two-factor authentication bagi seluruh akun, pembentukan tim kepatuhan UU PDP yang bertugas melakukan audit berkala, implementasi Disaster Recovery Plan yang diuji secara rutin, serta peningkatan transparansi kebijakan privasi kepada pengguna.

4. KESIMPULAN

Berdasarkan hasil analisis privasi data pengguna Shopee menggunakan framework ISO 31000:2018, dapat ditarik kesimpulan sebagai berikut:

1. Identifikasi risiko menghasilkan 8 risiko utama privasi data pengguna Shopee, yaitu kebocoran data pribadi (R1), pencurian akun pengguna (R2), penyalahgunaan hak akses karyawan (R3), pelanggaran UU PDP (R4), serangan ransomware (R5), pembobolan sistem pembayaran (R6), kehilangan data akibat server crash (R7), dan penjualan data ke pihak ketiga (R8).
2. Analisis risiko menunjukkan bahwa nilai frekuensi tertinggi (nilai 3) terdapat pada risiko pencurian akun pengguna (R2) dan kehilangan data akibat server crash (R7), sedangkan nilai dampak tertinggi (nilai 5) terdapat pada hampir semua risiko kecuali R2 dan R7 (nilai 4).
3. Evaluasi risiko menunjukkan bahwa seluruh risiko berada pada level Menengah dengan nilai tingkat risiko antara 5 hingga 12. Tidak ada risiko yang masuk kategori Tinggi (13-25) maupun Rendah (1-4).
4. Perlakuan risiko menghasilkan rekomendasi mitigasi untuk 7 risiko (mitigate) dan 1 risiko (accept). Risiko penjualan data ke pihak ketiga (R8) direkomendasikan untuk diterima dengan syarat Shopee transparan kepada pengguna.
5. Penerapan ISO 31000:2018 terbukti efektif sebagai framework untuk mengidentifikasi, menganalisis, mengevaluasi, dan memberikan rekomendasi perlakuan risiko privasi data secara sistematis dan terstruktur.

Keterbatasan penelitian ini adalah penggunaan data sekunder tanpa verifikasi langsung ke pihak Shopee. Penelitian mendatang disarankan melakukan pendekatan kuantitatif melalui survei kepada pengguna Shopee serta studi komparatif dengan platform e-commerce lainnya seperti Tokopedia dan Lazada [16], [18].

DAFTAR PUSTAKA

[1] T. A. Cahyaaty, I. Wijaya, M. Dafin, and A. Dzky, "Analisis Keamanan Data Pribadi Pada Pengguna E-Commerce Shopee Terhadap Ancaman Data Pribadi," vol. 5, no. 2, pp. 133–144, 2024, doi: https://doi.org/10.31599/mdpf3g55.

[2] Y. N. Silalahi and M. I. P. Nasution, "Tinjauan Sistem Keamanan Data Pelanggan di E-Commerce: Studi Kasus Platform Shopee," *J. Sist. Informasi, Manaj. dan Teknol. Inf.*, vol. 3, no. 2, pp. 113–122, 2025, doi: 10.33020/jsimtek.v3i2.813.

[3] D. T. Sonda, "Tinjauan Yuridis Tanggung Jawab Penyelenggara E-Commerce dalam Penyalahgunaan Data Pribadi oleh Pihak Ketiga dalam Transaksi Shopee Pay Later," Universitas Sumatera Utara, 2024.

[4] "UU No. 27 Tahun 2022." [Online]. Available: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

[5] R. Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?," *LAW REFORM*, vol. 18, no. 2, pp. 144–163, 2022, doi: 10.14710/lr.v18i2.43307.

[6] A. M. Chaniago, M. Siregar, and J. Arifiyanto, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi E-Commerce Shopee," *J. Sci. Soc. Res.*, vol. 8, no. 1, pp. 184–195, 2025.

[7] I. O. für Normung, *ISO 31000: 2018: Risk Management: Guidelines*. ISO, 2018.

[8] S. Yakin, T. Hasanuddin, and N. Kurniati, "Application of content based image retrieval in digital image search system," *Bull. Electr. Eng. Informatics*, vol. 10, no. 2, pp. 1122–1128, 2021, doi: 10.11591/EEI.V10I2.2713.

[9] A. Setiawan and R. Puspitadewi, "Challenges and Perspectives on Personal Risk Management and Data Privacy in the Indonesian Context," *Rev. Integr. Bus. Econ. Res.*, vol. 15, p. 3, 2026.

[10] Sulpawati, N. Choirunnisa, and H. F. Rohman, "Strategi Manajemen Risiko Operasional dalam Bisnis E-Commerce untuk Menghadapi Tantangan dan Menemukan Solusi," *J. Manaj. dan Pemasar. (Jump.)*, vol. 4, no. 1, 2025, doi: 10.51771/jumper.v4i1.1729.

[11] E. K. Usmany, "Information Security Planning with Risk Management Using ISO 31000:2018 at E-Commerce XYZ," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 33, pp. 75–89, 2025, doi: 10.52783/jisem.v10i33s.5460.

[12] A. P. Kehista *et al.*, "Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)," *J. Ilmu Manaj. Terap.*, vol. 4, no. 5, pp. 625–632, 2023, doi: 10.31933/JIMT.V4I5.1541.

[13] T. Sutabri, Y. Pratama, M. I. Herdiansyah, and W. Cholil, "Information Technology Risk Management Analysis Using COBIT and ISO at Jumputan Industry," *Int. J. Informatics Vis.*, vol. 9, no. 6, pp. 2418–2429, 2025, doi: 10.62527/JOIV.9.6.3236.

[14] A. Muhammad, C. P. T.W, R. Fauzi, and Pramono, "Efektivitas Platform E-Commerce Dalam Mendukung Bisnis Kaos Anime," *J. Inf. \& Comput.*, vol. 3, no. 1, pp. 21–31, 2025, doi: 10.32493/JICOMISC.V3I1.46981.

[15] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems," 2002. doi: https://doi.org/10.6028/NIST.SP.800-30.

[16] A. Ulya, A. Karima, T. S. A. Sukiman, A. Zulfia, and R. Rahmawati, "Information Security Risk Analysis Using ISO 31000:2018 and ISO 27001:2022," *Brill. Res. Artif. Intell.*, vol. 5, no. 2, pp. 843–853, 2025, doi: 10.47709/brilliance.v5i2.6564.

[17] T. M. Muhtar and E. Radhiansyah, "Analisis Implementasi Kebijakan Perlindungan Data Pribadi dalam Perdagangan Digital di Indonesia Berdasarkan eTrade Readiness Assessment," *J. Integr. Int. Relations*, vol. 10, no. 2, pp. 157–179, 2025, doi: 10.15642/jiir.2025.10.2.157-179.

[18] M. M. R. Akbar, K. Yudhistiro, and A. R. Muslikh, "Analysis of Tokopedia Digital Security Strategy Against Cyber Threats Using the Risk Assessment Framework Approach," *J. Innov. Comput. Sci.*, vol. 4, no. 2, pp. 94–101, 2025, doi: 10.56347/JICS.V4I2.301.

[19] F. S. Lubis, V. S. Praditha, M. Lubis, M. F. Safitra, and Y. Z. Ramadhan, "IT Risk Analysis Based on Risk Management Using ISO 31000: Case study Registration Application at University XYZ," *Proc. 2023 9th Int. Conf. Ind. Bus. Eng.*, pp. 522–528, 2023, doi: 10.1145/3629378.3629464.

[20] M. Ekania, E. Hamdi, R. Indradewa, and F. Abadi, "Risk Management Planning in E-Commerce Companies PT. SIMPEL OM UNGGULAN "SIMPEL OMâ€□," *Syntax Idea*, vol. 5, no. 11, pp. 1939–1956, 2023, doi: 10.46799/SYNTAX-IDEA.V5I11.2661.