MS-ECOM 001:2026

Multicert Standard MS-ECOM 001:2026

Wytyczne Programu Certyfikacji Sklepów Internetowych w zakresie zaufania konsumenta, bezpieczeństwa danych, zgodności z Digital Services Act, RODO i prawem konsumenckim.

Dokument bazowy: ISO 9001:2015 + RODO + Digital Services Act (UE 2022/2065) + dyrektywa Omnibus + PCI DSS v4.0
Schemat: Type 6 (certyfikacja systemu zarządzania) wg ISO/IEC 17067
Bezstronność: ISO/IEC 17021-1 + ISO/IEC 17065
Etap dojrzałości: Multicert Standard (rok 1) — ścieżka do CWA/PAS w roku 2-3

Wersja 1.0 · Kwiecień 2026

Multicert Sp. z o.o. · multicert.pl

STRONA WYDAWNICZA · PUBLICATION DETAILS

Multicert Standard MS-ECOM 001:2026

MS-ECOM 001:2026

TYTUŁ DOKUMENTU	Multicert Standard MS-ECOM 001:2026
KOD IDENTYFIKACYJNY	**MS-ECOM 001:2026**
WYDANIE	Wersja 1.0 · Kwiecień 2026
STATUS	Dokument normatywny — wytyczne audytowe programu certyfikacji
DATA WYDANIA	Kwiecień 2026
JĘZYK WYDANIA	Polski (pl)
DOKUMENT BAZOWY	ISO 9001:2015 + RODO + Digital Services Act (UE 2022/2065) + dyrektywa Omnibus + PCI DSS v4.0
SCHEMAT CERTYFIKACJI	Type 6 (certyfikacja systemu zarządzania) wg ISO/IEC 17067:2013
ZAKRES POWOŁAŃ	ISO/IEC 17021-1:2015 + ISO/IEC 17065:2012 + ISO 19011:2018

ZATWIERDZENIE DOKUMENTU

ZATWIERDZIŁ	**Grzegorz Suwara**
STANOWISKO	Prezes Zarządu Multicert Sp. z o.o.
DATA ZATWIERDZENIA	21 kwietnia 2026 r.
PODPIS	*Grzegorz Suwara*

WYDAWCA

Multicert Sp. z o.o.
ul. Mydlarska 47A, 04-690 Warszawa, Polska
Sąd Rejonowy dla m.st. Warszawy, XIII Wydział Gospodarczy KRS
KRS 0000681322 · NIP 9522163792 · REGON 367470425
multicert.pl · biuro@multicert.pl · +48 (22) 308 67 47

Spis treści

Załączniki dostępne jako osobne dokumenty: Załącznik A — Checklist audytora. Załącznik B — Wzory dokumentów. Załącznik C — Macierz wymagań × poziom certyfikatu.

1 Zakres

Niniejszy standard określa wymagania, procedurę oceny i kryteria wydania certyfikatu **Multicert E-commerce Trust** — programu certyfikacji sklepów internetowych w zakresie zaufania konsumenta, bezpieczeństwa danych, zgodności z Digital Services Act (DSA), RODO, dyrektywą Omnibus i innym prawem konsumenckim.

Program obejmuje certyfikację:

- **Sklepów B2C** — platformy własne (Magento, Shopify, WooCommerce, PrestaShop, Shoper, IdoSell), marketplaces własne, social commerce;
- **Marketplaces i agregatorów** — platformy łączące sprzedawców z konsumentami (Allegro, OLX, Empik, Grupa Amazon);
- **Sklepów B2B z panelem self-service** — gdzie element zakupu online pełni istotną rolę;

- **Platform D2C i subskrypcyjnych** — bezpośrednia sprzedaż producentów do konsumentów, modele abonamentowe.

Certyfikat daje konsumentowi obiektywny sygnał, że sklep spełnia wyższe standardy niż minimum prawne w zakresie: transparentności cenowej, ochrony danych osobowych, obsługi reklamacji, czasu dostawy, bezpieczeństwa płatności, rzetelności komunikacji marketingowej. Widoczny znak w checkout zwiększa conversion rate (badania 2023: +8–15 % vs sklepy bez znaku trust).

2 Powołania normatywne

Niniejszy dokument odwołuje się do następujących dokumentów (datowane wydania obowiązują w wymienionej formie; niedatowane — najnowsze wydanie):

- ISO 9001:2015 — Systemy zarządzania jakością
- ISO/IEC 27001:2022 — Systemy zarządzania bezpieczeństwem informacji
- ISO 10002:2018 — Zarządzanie jakością. Satysfakcja klienta. Wytyczne postępowania z reklamacjami
- ISO 19011:2018 — Wytyczne auditowania systemów zarządzania
- ISO/IEC 17021-1:2015 — Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania
- Rozporządzenie (UE) 2016/679 (RODO)
- Rozporządzenie (UE) 2022/2065 — Digital Services Act (DSA)
- Dyrektywa (UE) 2019/2161 — Omnibus (egzekwowanie praw konsumentów)
- Dyrektywa 2011/83/UE — prawa konsumentów
- PCI DSS v4.0 — Payment Card Industry Data Security Standard
- PSD2 (dyrektywa 2015/2366) — usługi płatnicze
- Ustawa z 30 maja 2014 r. o prawach konsumenta (Dz.U. 2014 poz. 827)
- Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000)
- Multicert Scheme Framework v1.0

3 Terminy i definicje

Dla celów niniejszego dokumentu obowiązują następujące terminy i definicje:

1. **E-commerce** — Handel elektroniczny — sprzedaż towarów i usług z wykorzystaniem internetu, platform cyfrowych, aplikacji mobilnych. W niniejszym standardzie obejmuje B2C, B2B z komponentem self-service, D2C, subskrypcje.
2. **Digital Services Act (DSA)** — Rozporządzenie (UE) 2022/2065 obowiązujące od 17 lutego 2024 r. dla wszystkich platform cyfrowych w UE. Ustanawia obowiązki przejrzystości, zarządzania ryzykiem, reagowania na nielegalne treści. VLOPs (Very Large Online Platforms, > 45 mln użytkowników miesięcznie) — obowiązki rozszerzone.
3. **Dyrektywa Omnibus** — Dyrektywa (UE) 2019/2161 wdrożona w Polsce od 1 stycznia 2023 r. Nakłada obowiązki transparentności cenowej (minimum cena z 30 dni przed promocją), weryfikacji opinii konsumentów, jasnych zasad rankingowania produktów.
4. **Customer Trust** — Zaufanie konsumenta — subiektywna percepcja wiarygodności sklepu oparta o elementy: rzetelność informacji, bezpieczeństwo płatności, ochrona danych, obsługa reklamacji, komunikacja. Mierzony przez NPS, CSAT, trust pilot score.
5. **Transparentność cenowa (Omnibus)** — Wymóg art. 5a Dyrektywy 2019/2161 — przy promocji cenowej sprzedawca musi podać najniższą cenę z 30 dni przed obniżką. Nieprzestrzeganie: kary do 10 % obrotu.
6. **PCI DSS v4.0** — Standard bezpieczeństwa kart płatniczych wydawany przez PCI Security Standards Council. Wymagany dla wszystkich organizacji przechowujących, przetwarzających lub transmitujących dane kart. Od marca 2025 r. v4.0 zastąpiła v3.2.1.
7. **Chargeback** — Obciążenie zwrotne — cofnięcie transakcji kartową przez bank konsumenta na jego żądanie (kwestionowanie transakcji). Wskaźnik chargeback ratio monitorowany przez operatorów — przekroczenie 1 % skutkuje karami i ryzykiem utraty możliwości przyjmowania płatności.
8. **Anti-fraud** — System wykrywania i zapobiegania oszustwom płatniczym — 3D Secure, behavioural biometrics, device fingerprinting, velocity checks, blacklists. Integrowany z procesorem płatności (PayU, Przelewy24, Stripe, itp.).
9. **Reklamacja (complaint)** — Zgodnie z Kodeksem Cywilnym i Ustawą o prawach konsumenta — żądanie konsumenta obniżki ceny, wymiany, naprawy lub zwrotu za wadliwą rzecz/usługę. Sprzedawca ma 14 dni na odpowiedź.
10. **Zwrot (right of withdrawal)** — Prawo odstąpienia od umowy w terminie 14 dni (art. 27 Ustawy o prawach konsumenta). Konsument może zwrócić towar bez podania przyczyny, sprzedawca zwraca pieniądze w 14 dni.
11. **Dispute resolution** — Rozwiązywanie sporów — ścieżki: bezpośrednio między sprzedawcą a konsumentem, przez platformę ODR (Online Dispute Resolution) KE, przez arbitraż branżowy

(UOKiK, Inspekcja Handlowa).

12. **Multicert E-commerce Trust** — Autorski program certyfikacji sklepów internetowych Multicert Sp. z o.o. kod MS-ECOM 001:2026.

13. **Certyfikat Multicert E-commerce Trust** — Dokument wydany przez Multicert Sp. z o.o. potwierdzający zgodność sklepu internetowego z MS-ECOM 001:2026. Numer MC-ECOM-RRRR-NNNN, zakres (domeny, platformy), poziom (Essential/Advanced/Leader), okres ważności 3 lata. Widoczny znak trust do wyświetlania w checkout i footer.

3A Skróty

SKRÓT	ROZWINIĘCIE
B2B	Business-to-Business
B2C	Business-to-Consumer
D2C	Direct-to-Consumer
DSA	Digital Services Act
DSAR	Data Subject Access Request (wniosek o dostęp do danych wg RODO)
MS-ECOM	Multicert Standard — E-commerce Trust
NPS	Net Promoter Score
ODR	Online Dispute Resolution
PCI DSS	Payment Card Industry Data Security Standard
PSD2	Payment Services Directive 2
RODO	Rozporządzenie (UE) 2016/679 o Ochronie Danych Osobowych (GDPR)
SLA	Service Level Agreement
VLOP	Very Large Online Platform (DSA)

4 Zakres programu i kwalifikacja sklepu

Bazuje na: ISO 9001 §4 + DSA

4.1 Zakres rzeczowy

Program **Multicert E-commerce Trust** obejmuje certyfikację sklepów internetowych prowadzących sprzedaż towarów lub usług w modelu B2C, B2B self-service, D2C, subskrypcyjnym. Wymaganie wstępne: minimum 12 miesięcy działania, formalna rejestracja (KRS/CEIDG), aktywna obsługa klienta.

4.2 Zakres certyfikacji

Zakres określa:

- Domeny i subdomeny objęte certyfikatem (www, m.sklep, app, kasa);
- Platformy (webstore, aplikacja mobilna, marketplace ID);
- Kanały sprzedaży (online, omnichannel, social commerce);
- Kategorie produktów (może być wyłączenie — np. produkty dla dorosłych, alkohol, broń).

4.3 Wyłączenia z programu

- Sklepy sprzedające produkty sprzeczne z prawem polskim/UE;
- Platformy hazardowe bez licencji Ministra Finansów;
- Sklepy z produktami regulowanymi odrębnymi przepisami (farmaceutyczne, medyczne — osobne schematy sektorowe);
- Sklepy z nieaktualnym regulaminem lub niezgodnym z prawem konsumenckim.

5 Wymagania dla sklepu

Bazuje na: RODO + DSA + Omnibus + PCI DSS + prawo konsumenckie

5.1 Transparentność i zgodność prawna

- **Regulamin sklepu** zgodny z Ustawą o prawach konsumenta, dostępny przed zakupem, zaakceptowany przez checkbox;
- **Polityka prywatności (RODO)** — cele przetwarzania, podstawa prawna, czas retencji, prawa konsumenta, DPO kontakt;
- **Transparentność cenowa (Omnibus)** — przy promocji widoczna najniższa cena z 30 dni przed obniżką;
- **Weryfikacja opinii** — jeśli publikowane opinie konsumentów, muszą być od rzeczywistych kupujących (mechanizm weryfikacji);
- **Zasady rankingowania produktów** — jawne kryteria (cena, popularność, sponsorowane);
- **Kontakt do sprzedawcy** — nazwa, adres, NIP, REGON, email, telefon widoczne w stopce.

5.2 Ochrona danych osobowych (RODO)

- Inwentarz danych osobowych — jakie kategorie, cele, odbiorcy, retencja;
- Zgody marketingowe — opt-in, łatwe odwołanie, oddzielnie od regulaminu;
- Procedura DSAR (Data Subject Access Request) — dostęp, poprawa, usunięcie, przenośność;
- Ochrona techniczna — TLS 1.2+, hashed passwords (bcrypt/argon2), access controls;
- Naruszenia danych — procedura zgłoszenia do UODO w 72 h;
- DPO (Data Protection Officer) — wymagany dla VLOP-grade, zalecany dla Advanced/Leader;
- Polityka cookie — zgody granulowane, łatwe odwołanie, kategoryzacja cookies.

5.3 Bezpieczeństwo płatności (PCI DSS)

- Zgodność z PCI DSS odpowiednim do skali (SAQ A/B/C/D wg schematu flag);
- Brak przechowywania danych kart (CVV nigdy, PAN maskowany po pierwszej 6 ostatnich 4);
- Integracja z certyfikowanym procesorem płatności (PayU, Przelewy24, Stripe, Adyen);
- 3D Secure v2 dla wszystkich transakcji;
- Anti-fraud system — monitoring, blacklists, velocity, device fingerprinting;
- Chargeback ratio monitorowany, target < 0,5 %.

5.4 Obsługa klienta i reklamacji (ISO 10002)

- Kanały kontaktu — email, telefon, chat, formularz — dostępne i działające;
- SLA odpowiedzi — email < 24 h robocze, chat < 5 min w godzinach obsługi, telefon < 3 dzwonków;
- Procedura reklamacji — formalna ścieżka, potwierdzenie otrzymania, decyzja w 14 dni;
- Procedura zwrotów — 14 dni na odstąpienie, zwrot pieniędzy w 14 dni od otrzymania zwrotu;
- Rejestr reklamacji i zwrotów — analiza przyczyn, trendy, działania systemowe;

- Mierzenie satysfakcji klienta — NPS lub CSAT minimum raz w roku.

5.5 Digital Services Act – wymagania

- Terms & Conditions zgodne z DSA — jasny język, jednoznaczne zasady moderowania treści;
- Mechanizm notice-and-action dla nielegalnych treści (jeśli platforma z UGC);
- Jawność reklam — kto finansuje, dlaczego wyświetlone, kryteria targetowania;
- Roczny raport przejrzystości (dla marketplaces i platform z UGC) — statystyki moderacji, zgłoszenia, decyzje;
- VLOP-grade (dla Leader > 45 mln MAU) — risk assessment, niezależny audyt, compliance officer.

5.6 Dostawa, logistyka, zwroty

- Deklarowany czas dostawy widoczny przed zakupem — z dokładnością ≥ 1 dzień roboczy;
- Tracking zamówienia dostępny dla klienta — nr przesyłki, status, estymowany termin;
- Opcje dostawy — minimum 3 alternatywy (kurier, paczkomat, odbiór osobisty);
- Informacja o kosztach dostawy przed checkout — bez ukrywania;
- Proces zwrotu — formularz online, etykieta zwrotna, partner logistyczny dla zwrotów.

5.7 Ciągłość działania i bezpieczeństwo techniczne

- Uptime > 99,5 % rocznie (Advanced/Leader > 99,9 %);
- Backup danych — codzienne, retencja ≥ 30 dni, testowany restore;
- Disaster Recovery Plan — RTO/RPO zdefiniowane;
- Monitoring wydajności (page speed, error rates, conversion funnel);
- Dla Advanced/Leader — SOC lub równoważny MDR.

5.8 Komunikacja marketingowa

- Newsletter z wyraźnym opt-in, opt-out w każdym wysyłce, respekt list Robinson;
- Influencer marketing — oznaczanie #reklama, #sponsorowane wg wytycznych UOKiK;
- Email marketing zgodny z RODO + ustawą o świadczeniu usług drogą elektroniczną;
- Brak cen pułapek, dark patterns, misleading claims.

6 Procedura oceny i wydania certyfikatu

Bazuje na: ISO/IEC 17021-1:2015

6.1 Etap 1 – Wniosek i kwalifikacja (3–5 dni)

Sklep składa wniosek przez **multicert.pl/kontakt** z dopiskiem „*E-commerce Trust — MS-ECOM 001*". Wymagane: domena, platforma, obrót roczny, liczba transakcji.

6.2 Etap 2 – Audyt Stage 1 (1–2 dni)

Audytor wiodący + ekspert e-commerce/prawnik (RODO + prawo konsumenckie). Przegląd zdalny: regulamin, polityka prywatności, compliance Omnibus, struktura strony.

6.3 Etap 3 – Audyt Stage 2 (2–8 dni, zdalnie + on-site HQ)

Pełny audyt: przegląd backend (dostęp do CMS, logi, systemu reklamacji), test transakcji (zakup + zwrot), wywiady z zespołami (obsługa klienta, IT, legal, marketing), przegląd rejestrów incydentów.

6.4 Etap 4 – Raport i korekty (30–90 dni)

6.5 Etap 5 – Decyzja komisji (2 tygodnie)

Komisja Multicert + prawnik konsumencki + ekspert IT security.

6.6 Etap 6 – Wydanie certyfikatu i znaku trust (1 tydzień)

Certyfikat MC-ECOM-RRRR-NNNN + kod embed znaku trust (badge HTML/JavaScript dla checkout i footer). Audyty nadzorcze: Essential 1 × rocznie + mystery shopping 2 × rocznie (niezapowiedziane); Advanced 1 × rocznie + 4 × mystery shopping; Leader 2 × rocznie + ciągły monitoring via crawler.

7 Procedura audytu

Etap 0 – Kwalifikacja (3–5 dni)

Etap 1 – Umowa certyfikacyjna (1 tydzień)

Etap 2 – Stage 1 readiness review (1–2 dni)

Etap 3 – Stage 2 certification audit (2–8 dni)

Etap 4 – Raport i działania korygujące (30–90 dni)

Etap 5 – Decyzja komisji certyfikacyjnej (2 tygodnie)

Etap 6 – Wydanie certyfikatu i kodu znaku trust (1 tydzień)

Nadzór (3 lata ważności)

Essential — 1 audyt + 2 × mystery shopping rocznie; Advanced — 1 audyt + 4 × mystery shopping; Leader — 2 audyty + ciągły monitoring via crawler Multicert.

8 Czas audytu (person-days)

Tabela poniżej określa minimalny nakład pracy audytora dla pełnego cyklu certyfikacyjnego (Etap 1 + Etap 2 + Anonymous Survey). Czas dostosowywany do rzeczywistej dojrzałości i złożoności systemu.

WIELKOŚĆ	ESSENTIAL	ADVANCED	LEADER
Mały sklep (< 5 mln zł obrotu, 1 platforma)	2 person-days	4 person-days	6 person-days
Średni sklep (5–50 mln zł, 2–3 platformy)	4 person-days	6 person-days	10 person-days
Duży sklep / marketplace (> 50 mln zł)	6 person-days	10 person-days	16 person-days
VLOP (> 45 mln MAU, platforma z UGC)	10 person-days	16 person-days	24 person-days + ciągły monitoring

9 Próbkowanie

- **Test zakupu** — audytor dokonuje 3–5 testowych zakupów (różne kategorie, metody płatności, dostawy);
- **Test zwrotu** — minimum 2 zwroty z każdej kategorii produktów;
- **Rejestr reklamacji** — próba 20–50 reklamacji z cyklu 12 miesięcy (różne kategorie, typy, klienci);
- **Rejestr DSAR** — wszystkie wnioski z ostatnich 12 miesięcy + dowody realizacji;
- **Rejestr incydentów** — incydenty bezpieczeństwa, naruszenia RODO, fraud, chargebacks;
- **Wywiady** — min. kierownik sklepu, odpowiedzialny za IT, DPO, menedżer obsługi klienta, legal;
- **Mystery shopping** — 2–12 razy rocznie (zależnie od poziomu), audyt bez zapowiedzi.

10 Kryteria oceny i klasyfikacja niezgodności

OBSZAR	WAGA	ŹRÓDŁO OCENY
Transparentność i compliance prawne	25%	Regulamin, Omnibus, DSA, RODO — przegląd + test
Bezpieczeństwo płatności i danych	25%	PCI DSS, RODO, TLS, incident history
Obsługa klienta i reklamacji	20%	SLA, ISO 10002, CSAT, rejestr reklamacji
Dostawa i zwroty	15%	Test zakupu, tracking, SLA, opcje
Ciągłość i niezawodność	15%	Uptime, DR plan, monitoring, incydenty

Klasyfikacja niezgodności

- **Major** — poważne naruszenie prawa (brak polityki RODO, łamanie Omnibus, ujawnienie danych kart, blokowanie zwrotów). Wdrożenie natychmiastowe.
- **Minor** — pojedyncze odchylenie. Plan korekt.
- **OFI** — sugestia doskonalenia.

Progi decyzyjne

- Wydanie: 0 Major + ≤ 8 Minor + ocena ogólna ≥ 75%
- Warunkowe: 0 Major + 9–15 Minor (60 dni korekt)
- Odmowa: ≥ 1 Major niewyjaśniona w 90 dni lub > 15 Minor
- Odroczenie: 60–74%

11 FAQ (najczęstsze pytania) i glossary (słownik pojęć)

FAQ (Frequently Asked Questions – najczęstsze pytania)

Czy certyfikat Multicert E-commerce Trust to Trusted Shops?
Nie. Trusted Shops to komercyjny znak niemiecki. Multicert E-commerce Trust jest polskim programem, wydawanym przez akredytowaną jednostkę certyfikującą, z ramami ISO/IEC 17065. Różni się zakresem (pełna mapa DSA + Omnibus + PCI DSS + RODO).

Ile kosztuje certyfikacja i jak długo trwa?
Essential: 15–40 tys. zł. Advanced: 40–100 tys. zł. Leader: 80–200 tys. zł dla dużych marketplaces. Czas: 14–20 tygodni od wniosku.

Czy mogę używać znaku trust przed wydaniem certyfikatu?
Nie. Znak trust jest integralną częścią certyfikatu i udostępniany (jako kod HTML + badge) dopiero po pozytywnej decyzji komisji.

Jak certyfikat wpływa na conversion rate?
Badania 2023 (German Retail E-commerce Monitor, Baymard Institute, Trustpilot) pokazują wzrost 8–15 % dla sklepów z widocznym znakiem trust certyfikowanej jednostki, szczególnie w segmencie 100–500 zł koszyka.

Czy program obejmuje sklepy na Allegro / Amazon?
Tak — osobny zakres dla marketplace sellers. Certyfikat potwierdza compliance sprzedawcy, nie platformy. Dla operatorów platform (Allegro, OLX) — osobny tier Leader z oceną jako VLOP.

Czy muszę być zgodny z DSA jeśli jestem małym sklepem?
Tak — DSA stosuje się do wszystkich platform cyfrowych (hosting services, intermediaries). Małe sklepy (B2C własne produkty) mają ograniczone obowiązki, ale nie są wyłączone. Essential pokrywa minimum.

Glossary (słownik pojęć)

1. **DSA** — Digital Services Act — rozporządzenie UE 2022/2065 o jednolitym rynku usług cyfrowych.
2. **Omnibus** — Dyrektywa 2019/2161 o lepszym egzekwowaniu praw konsumentów — transparentność cenowa, weryfikacja opinii.
3. **VLOP** — Very Large Online Platform — platformy z > 45 mln użytkowników miesięcznie w UE, rozszerzone obowiązki DSA.
4. **DSAR** — Data Subject Access Request — wniosek osoby fizycznej o dostęp do swoich danych wg RODO.
5. **PCI DSS** — Payment Card Industry Data Security Standard — standard bezpieczeństwa kart.
6. **SAQ** — Self-Assessment Questionnaire — kwestionariusz samooceny PCI DSS zależny od sposobu przyjmowania płatności.

7. **Chargeback** — Obciążenie zwrotne — cofnięcie transakcji kartową przez bank konsumenta.

12 Bibliografia

Niniejsza bibliografia zawiera pełne odniesienia do dokumentów źródłowych wykorzystanych przy opracowaniu standardu. Format zgodny z ISO 690:2021 *Information and documentation — Guidelines for bibliographic references and citations*.

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 9001:2015. Quality management systems — Requirements.* Geneva: ISO, 2015.

[2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27001:2022. Information security management systems — Requirements.* Geneva: ISO, 2022.

[3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 10002:2018. Quality management — Customer satisfaction — Guidelines for complaints handling in organizations.* Geneva: ISO, 2018.

[4] PARLAMENT EUROPEJSKI I RADA. *Rozporządzenie (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).* Dz.U. UE L 119, 4.5.2016.

[5] PARLAMENT EUROPEJSKI I RADA. *Rozporządzenie (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych (Digital Services Act).* Dz.U. UE L 277, 27.10.2022.

[6] PARLAMENT EUROPEJSKI I RADA. *Dyrektywa (UE) 2019/2161 z dnia 27 listopada 2019 r. w sprawie lepszego egzekwowania praw konsumentów (Omnibus).* Dz.U. UE L 328, 18.12.2019.

[7] PCI SECURITY STANDARDS COUNCIL. *PCI DSS v4.0. Payment Card Industry Data Security Standard.* Wakefield: PCI SSC, 2022.

[8] SEJM RZECZYPOSPOLITEJ POLSKIEJ. *Ustawa z dnia 30 maja 2014 r. o prawach konsumenta.* Dz.U. 2014 poz. 827, z późn. zm.

[9] MULTICERT SP. Z O.O. *Multicert Scheme Framework v1.0.* Warszawa: Multicert, 2026.

13 Kontakt i wniosek

PEŁNOMOCNIK KLIENTA

Joanna Kałuża
Doradca ds. certyfikacji Multicert E-commerce Trust
Tel: **+48 508 354 544**
Email: **joanna.kaluza@multicert.pl**

MULTICERT SP. Z O.O.

ul. Mydlarska 47A, 04-690 Warszawa
NIP 9522163792
multicert.pl

Wniosek o certyfikację: formularz na multicert.pl/kontakt z dopiskiem „Multicert E-commerce Trust — Program Certyfikacji Sklepów Internetowych — wytyczne MS-ECOM 001:2026".