

OBOWIĄZEK INFORMACYJNY (Akt w sprawie danych – „Data Act”)

Od 12 września 2025 r. sprzedawca ma obowiązek informować, jak urządzenia skomunikowane i powiązane usługi przetwarzają dane. Laptop jest urządzeniem skomunikowanym (łączy się z siecią, usługami producenta i aktualizacjami), a część funkcji zapewniają usługi powiązane (aplikacje systemowe i narzędzia producenta).

Link: <https://digital-strategy.ec.europa.eu/pl/factpages/data-act-explained> [11.09.2025]

Podmiot sporządzający / sprzedawca

DRAUG – Sebastian Stręciwilk

NIP: 9223080348 | VAT: PL9223080348 | REGON: 527863227

Strona Internetowa: www.draug.pl

Adres: ul. Tomasza Zana 43/2.1, 20-601 Lublin (Śródmieście)

Telefon: +48 502 485 952 | E-mail: kontakt@draug.pl

Sprzedaż online: terytorium Polski Profil działalności: sprzedaż laptopów poleasingowych, usługi IT (diagnoza, drobne naprawy, strony WWW, wsparcie IT)

Dzień założenia działalności: 11.03.2024

Nr rachunku bankowego (IBAN): PL86 1050 1953 1000 0090 8341 1042

Klauzula autorska i integralność oferty Niniejszy dokument został przygotowany wyłącznie dla ofert sklepu DRAUG i stanowi ich integralną część.

CO TO SĄ DANE I PO CO SĄ PRZETWARZANE

- Zapewnienie aktualizacji i bezpieczeństwa (Windows, Defender, aktualizacje sterowników/BIOS).
- Usprawnienia jakości i diagnostyka (anonimowe lub zidentyfikowane dane użycia – zależnie od ustawień).
- Funkcje chmurowe i synchronizacja (np. OneDrive, konto Microsoft – tylko jeśli użytkownik je włączy).

Link: <https://www.microsoft.com/pl-pl/privacy/privacystatement> [11.09.2025]

SYSTEM: WINDOWS 11

Windows 11 przetwarza dane diagnostyczne i bezpieczeństwa w celu działania systemu (aktualizacje, wykrywanie błędów, ochrona). Zakres i wysyłanie danych można kontrolować w Ustawienia > Prywatność i zabezpieczenia (diagnostyka, uprawnienia aplikacji, historia aktywności). Szczegóły: Microsoft Privacy Statement i przewodnik dot. prywatności/diagnostyki. Microsoft Defender (wbudowany antywirus) analizuje pliki, procesy i połączenia sieciowe na potrzeby ochrony — szczegóły zakresu danych i przechowywania opisano w dokumentacji Defender.

Link: <https://www.microsoft.com/pl-pl/privacy/privacystatement> [11.09.2025]

Link: <https://learn.microsoft.com/pl-pl/windows/privacy/configure-windows-diagnostic-data-in-your-organization> [11.09.2025]

Link: <https://learn.microsoft.com/pl-pl/defender-endpoint/microsoft-defender-antivirus-windows> [11.09.2025]

DOMYŚLNE APLIKACJE WINDOWS

Microsoft Edge, Microsoft Store, Notatnik, Paint, narzędzia systemowe — działają lokalnie; część funkcji (np. sklep, synchronizacja profilu, OneDrive) wymaga konta i może przetwarzać dane w chmurze, jeśli użytkownik to włączy.

Link: <https://www.microsoft.com/pl-pl/windows/comprehensive-security> [11.09.2025]

DODATKOWE OPROGRAMOWANIE (zainstalowane)

Mozilla Firefox — przetwarza dane techniczne i ustawienia przeglądarki; zaawansowane opcje ochrony prywatności wbudowane.

Link: <https://www.mozilla.org/pl/privacy/firefox/> [11.09.2025]

Google Chrome — przetwarzanie zgodne z Polityką prywatności Google; szczegóły „Prywatność w Chrome” w Centrum pomocy.

Link: <https://policies.google.com/privacy?hl=pl-pl> [11.09.2025]

Brave — przeglądarka z ochroną prywatności; m.in. Safe Browsing z lokalną bazą skrótów adresów, blokowanie trackerów.

Link: <https://brave.com/privacy/browser/> [11.09.2025]

VLC — odtwarzacz multimedialny; działa lokalnie. Opcjonalnie może łączyć się z internetem, by pobierać metadane okładek/infos (można wyłączyć w preferencjach — „Allow metadata network access / Prywatność i dostęp do sieci”).

Link: <https://www.videolan.org/vlc/privacy.html> [11.09.2025]

Pakiet kodeków (Codec Pack) — komponenty do lokalnego dekodowania audio/wideo; brak konta/chmury.

LibreOffice — pakiet biurowy; dokumenty przetwarzane lokalnie (sam program nie wymaga konta). Polityka prywatności dotyczy m.in. stron i usług TDF.

Link: <https://www.libreoffice.org/about-us/privacy/privacy-policy-en/> [11.09.2025]

Biblioteki systemowe: .NET Framework, Microsoft Visual C++ Redistributables — składniki uruchomieniowe; nie zbierają danych o użytkowniku jako samodzielne usługi. (Ogólna polityka Microsoft dot. produktów).

Link: <https://www.microsoft.com/pl-pl/privacy/privacystatement> [11.09.2025]

Microsoft Defender — ochrona w czasie rzeczywistym; przetwarza sygnały bezpieczeństwa (np. metadane plików, hashe, informacje o procesach/sieci).

<https://learn.microsoft.com/pl-pl/defender-endpoint/microsoft-defender-antivirus-windows> [11.09.2025]

APLIKACJE WSPARCIA PRODUCENTA (instalujemy odpowiednio do marki sprzętu)

HP – HP Support Assistant / HP Perform: automatyczne wsparcie, aktualizacje, diagnostyka. HP może zbierać dane o konfiguracji, stanie i wydajności urządzenia, aby dobierać aktualizacje i rozwiązywać problemy; zakres i podstawy opisuje HP Privacy Statement oraz komunikaty danych dla modułów (np. Perform).

Link: <https://www.hp.com/us-en/ai-solutions/perform-faq-data-notice.html> [11.09.2025]

Link: <https://www.hp.com/content/dam/sites/worldwide/privacy/pdf/statement-2021/HP-Privacy-Statement-2021-pl.pdf> [11.09.2025]

Link: <https://www.hp.com/us-en/privacy/privacy-central.html> [11.09.2025]

Dell – SupportAssist: zbiera informacje o systemie (konfiguracja, stan, dzienniki) na potrzeby proaktywnej diagnostyki i wsparcia; ustawienia prywatności dostępne w aplikacji (Settings > Privacy and terms). Dodatkowe dokumenty: przewodnik i materiały bezpieczeństwa Dell.

Link: <https://www.dell.com/support/manuals/pl-pl/dell-supportassist-pcs-tablets/sahomepcs Ug/privacy-and-terms> [11.09.2025]

Link: <https://www.dell.com/support/manuals/pl-pl/dell-supportassist-servers-v1.2/dsasug/data-collected-by-supportassist> [11.09.2025]

Link: <https://www.delltechnologies.com/asset/pl-pl/services/support/industry-market/supportassist-for-business-pcs-security-white-paper.pdf> [11.09.2025]

Lenovo – Lenovo Vantage / Commercial Vantage: może zbierać identyfikatory urządzenia, zdarzenia i dane użycia aplikacji oraz (jeśli włączysz aktualizacje wg lokalizacji/sieci) info o Wi-Fi/VPN; przechowuje dane na PC i udostępnia Lenovo tylko przy wyrażeniu zgody („opt-in”). Zbieranie można wyłączyć w ustawieniach Vantage („Pomóż ulepszać” / usage statistics).

Link: <https://www.lenovo.com/pl/pl/privacy/> [11.09.2025]

TWOJE WYBORY I KONTROLA [System Windows]

Windows 11: Ustawienia > Prywatność i zabezpieczenia – diagnostyka, uprawnienia aplikacji (kamera, mikrofon, lokalizacja), historia aktywności.

Konta/Chmura: logowanie do kont producentów (Microsoft/Google/etc.) jest opcjonalne; brak logowania ogranicza przesyłanie danych konta.

Link: <https://www.microsoft.com/pl-pl/privacy/privacystatement> [11.09.2025]

Aplikacje producentów (HP/Dell/Lenovo): w aplikacji znajdziesz zakładkę Prywatność/Privacy; można tam ograniczyć lub wyłączyć wysyłanie danych diagnostycznych.

Przeglądarki: w ustawieniach prywatności można wyłączyć synchronizację, historię, personalizację i funkcje ochrony w chmurze (np. skanowanie adresów URL).

VLC: jeśli nie chcesz pobierania metadanych/folder artów z sieci, wyłącz w Preferencje > Prywatność i dostęp do sieci.

INFORMACJE O PRZETWARZANIU DANYCH – OFICJALNE ŹRÓDŁA

Microsoft (Windows/Defender): <https://www.microsoft.com/privacy/privacystatement>

Windows – diagnostyka/prywatność (IT/adm.): <https://learn.microsoft.com/windows/privacy/configure-windows-diagnostic-data-in-your-organization>

Mozilla Firefox – Privacy Notice: <https://www.mozilla.org/privacy/firefox/>

Google – Polityka prywatności: <https://policies.google.com/privacy>

Chrome – Prywatność w Chrome (pomoc): <https://support.google.com/chrome/answer/14225066>

Brave – Browser Privacy Policy: <https://brave.com/privacy/browser/>

LibreOffice – Privacy Policy (TDF): <https://www.libreoffice.org/about-us/privacy/privacy-policy-en/>

VLC – „Privacy & Network Access” (informacja techniczna): <https://www.videolan.org/vlc/privacy.html>

K-Lite Codec Pack – strona projektu: <https://codecguide.com/>

HP – Privacy Statement: <https://www.hp.com/us-en/privacy/privacy.html>

HP Perform – FAQ/Data Notice: <https://www.hp.com/us-en/ai-solutions/perform-faq-data-notice.html>

Dell – SupportAssist (Privacy & terms – wskazówki w aplikacji): <https://www.dell.com/support/manuals/en-us/dell-supportassist-pcs-tablets/sahomepcs Ug/privacy-and-terms>

Dell – Privacy Center: <https://www.dell.com/en-us/lp/privacy-center>

Lenovo – Privacy Statement (Vantage): <https://www.lenovo.com/us/en/privacy/>

WAŻNE UWAGI PRAKTYCZNE DLA KUPUJĄCEGO

Wszystkie preinstalowane programy działają w wersjach aktualnych na dzień sprzedaży.

Nic nie wymaga konta ani synchronizacji w chmurze, dopóki użytkownik sam tego nie włączy (np. logowanie do konta Microsoft/Google, włączenie OneDrive lub telemetrii w aplikacjach producenta).

Z poziomu systemu i każdej aplikacji można ograniczyć lub wyłączyć zbieranie danych zgodnie z linkami powyżej.

DODATKOWA PODSTAWA PRAWNA (Data Act)

Unijny „Akt w sprawie danych” wchodzi do zastosowania 12.09.2025 i dotyczy m.in. transparentności przetwarzania danych przez produkty i usługi powiązane. (Patrz: strona KE „Data Act explained”).

Link: <https://digital-strategy.ec.europa.eu/pl/factpages/data-act-explained>

DOSTĘP I PRZENOSZENIE DANYCH

Masz prawo uzyskać kopię danych generowanych podczas korzystania z produktu/usługi skomunikowanej oraz zlecić ich przekazanie wskazanej przez Ciebie osobie trzeciej. Udostępnienie danych użytkownikowi jest **nieodpłatne**.

ZAKRES DANYCH, CZĘSTOTLIWOŚĆ I WOLUMEN

Dane obejmują m.in. sygnały diagnostyczne i bezpieczeństwa systemu, zdarzenia aplikacji producenta oraz – jeśli włączysz – funkcje chmurowe i synchronizację. Częstotliwość zbierania i szacunkowy wolumen zależą od Twoich ustawień (np. poziom diagnostyki w Windows, moduły HP/Dell/Lenovo, synchronizacja w przeglądarkach). Przykładowo: zdarzenia bezpieczeństwa rejestrowane są w czasie rzeczywistym, statystyki użycia – okresowo.

POSIADACZ DANYCH I ADRESACI WNIOSKU

Posiadaczem danych jest zazwyczaj producent sprzętu lub dostawca powiązanej usługi (np. Microsoft dla Windows/Defender, HP/Dell/Lenovo dla aplikacji wsparcia, wydawca przeglądarki). Wnioski o dostęp/przekazanie kieruj bezpośrednio do danego podmiotu – odnośniki do polityk i ustawień znajdziesz w sekcji „INFORMACJE O PRZETWARZANIU DANYCH – OFICJALNE ŹRÓDŁA”.

JAK ZŁOŻYĆ WNIOSEK

Zgłoszenie składasz przez formularze prywatności lub kanały kontaktu wskazane przez posiadacza danych (linki w niniejszym dokumencie). **Sprzedawca nie pośredniczy** w składaniu wniosków; użytkownik składa je **samodzielnie u posiadaczy danych**.

Jak uzyskać dane samodzielnie

1. Zidentyfikuj posiadaczy danych

Spisz, z jakich elementów korzystasz na tym urządzeniu:

- system i zabezpieczenia (np. Windows / Defender),
- aplikacje producenta sprzętu (np. HP/Dell/Lenovo – narzędzia wsparcia),
- przeglądarki (Chrome/Edge/Firefox) i konta chmurowe (np. Microsoft/Google),
- inne usługi powiązane (np. synchronizacja, kopie zapasowe).

2. Zbierz identyfikatory potrzebne do wniosku

- adres e-mail konta (Microsoft/Google/Firefox),
- **model i numer seryjny/Service Tag** urządzenia,
- opcjonalnie: nazwa urządzenia w systemie, identyfikator urządzenia w aplikacji producenta, zakres dat, który Cię interesuje.

3. Złóż wniosek o dostęp/przeniesienie danych u każdego posiadacza

Wejdź w sekcje „Prywatność”/„Privacy” danego dostawcy (panel konta lub ustawienia aplikacji) i wybierz **żądanie dostępu do danych/eksport danych lub przeniesienie do osoby trzeciej**.

Jeśli w aplikacji nie ma przycisku „export”, złóż wniosek z poziomu formularza kontaktowego „Privacy/DSR”.

Sprzedawca nie pośredniczy w składaniu wniosków; użytkownik składa je **samodzielnie u posiadaczy danych**.

4. Wybierz format i zakres

Poproś o **powszechny format do odczytu maszynowego** (np. JSON lub CSV) i wskaż (z **wyłączeniem strażników dostępu – DMA**):

- kategorie danych (diagnostyka, zdarzenia bezpieczeństwa, dane aplikacji producenta, dzienniki serwisowe),
- **okres** (np. ostatnie 12 miesięcy),
- **częstotliwość** (zdarzenia w czasie rzeczywistym, logi okresowe – jeśli to możliwe w rozbiciu).

5. (Opcjonalnie) wskaż osobę trzecią do przeniesienia

Jeśli chcesz, aby dane trafiły bezpośrednio do wskazanego podmiotu, podaj w treści:

- nazwę i dane kontaktowe odbiorcy,
- podstawę prawną/umowną współpracy (jeśli wymagana),
- preferowany sposób przekazania (bezpieczny link, SFTP, szyfrowana paczka).

6. Potwierdź tożsamość i odbierz paczkę

Dostawca może poprosić o dodatkową weryfikację (np. kod z e-maila/logowanie do konta). Po potwierdzeniu otrzymasz paczkę z danymi lub informację o gotowym pobraniu.

7. Gdzie tego szukać – przykłady ścieżek

- **Microsoft (Windows/Defender/M365):** Panel prywatności konta → „Pobieranie danych konta” / „Zarządzaj danymi”; w samym Windows: Ustawienia → Prywatność i zabezpieczenia → Diagnostyka i opinie → **Przeglądarka danych diagnostycznych** (podgląd/eksport).
- **HP/Dell/Lenovo (narzędzia wsparcia):** Aplikacja producenta → Ustawienia → Prywatność/Diagnostyka

→ eksport/żądanie danych; jeśli brak opcji w aplikacji — skorzystaj z formularza „Privacy” producenta i podaj **numer seryjny/Service Tag**.

• **Przeglądarki i chmura:**

- **Google/Chrome:** centrum prywatności konta (eksport historii, aktywności i danych Chrome),
- **Microsoft/Edge:** panel prywatności konta (dane przeglądarki i usługi),
- **Firefox:** konto Firefox → ustawienia prywatności (dane synchronizacji, zakładki, historia jeśli była synchronizowana).

8. Koszt i czas

Udostępnienie danych użytkownikowi wchodzi w zakres **nieodpłatny**. Realizacja następuje **bez zbędnej zwłoki**; status wniosku sprawdzisz w panelu prywatności lub korespondencji e-mail.

WYŁĄCZENIA I OGRANICZENIA

Wywnioskowane lub pochodne treści (np. materiały audiowizualne, wysoko wzbogacone analizy) nie są objęte zakresem; w zakresie pozostają surowe dane generowane przez produkt/usługę (np. sygnały diagnostyczne, zdarzenia). Nie można wykorzystywać uzyskanych danych do tworzenia konkurencyjnego produktu skomunikowanego. W szczególnych przypadkach posiadacz danych może ograniczyć udostępnianie ze względu na ochronę tajemnic przedsiębiorstwa lub wymogi bezpieczeństwa produktu.

Posiadacz danych **nie jest zobowiązany** udostępniać danych osobom trzecim mającym siedzibę **poza UE**. Odmowa udostępnienia jest dopuszczalna **wyłącznie**, gdy posiadacz danych wykaże ryzyko **poważnej szkody gospodarczej** dla tajemnicy przedsiębiorstwa albo gdy udostępnienie naruszałoby **określone prawem** wymogi bezpieczeństwa produktu.

ZGODNOŚĆ Z RODO

Udostępnienie danych osobowych innemu podmiotowi wymaga odpowiedniej podstawy prawnej (np. zgody), zwłaszcza gdy wnioskodawca nie jest osobą, której dane dotyczą. Dane współtworzone mogą łączyć elementy osobowe i nieosobowe; stosujemy zasady minimalizacji i bezpieczeństwa.

SPORY I ODWOŁANIA

Spory na tle udostępniania danych można kierować do **certyfikowanych mechanizmów rozstrzygania sporów** (po ich wyznaczeniu w Polsce) lub do **właściwego organu** wyznaczonego na mocy Data Act.

Data: 12.09.2025

Podstawa prawna: Rozporządzenie (UE) 2023/2854 („Akt w sprawie danych”)

SŁOWNICZEK SKRÓTÓW I POJĘĆ

- **UE** – Unia Europejska.
- **KE** – Komisja Europejska.
- **Data Act** – Rozporządzenie (UE) 2023/2854 („Akt w sprawie danych”).
- **RODO** – Rozporządzenie (UE) 2016/679 (GDPR).
- **DMA** – Digital Markets Act (Akt o rynkach cyfrowych); „**strażnicy dostępu**” to platformy wyznaczone przez KE.
- **DSR** – *Data Subject Request* – wniosek o realizację praw osoby, której dane dotyczą (np. dostęp/eksport).
- **JSON** – *JavaScript Object Notation* – ustrukturyzowany, maszynowo czytelny format danych.
- **CSV** – *Comma-Separated Values* – tekstowy format danych tabelarycznych.
- **Eksport** (zamiast „export”) – polski zapis przeniesienia/wyprowadzenia danych do pliku lub do innego podmiotu.
- **SFTP** – *Secure File Transfer Protocol* – szyfrowany protokół transferu plików.

- **URL** – *Uniform Resource Locator* – adres internetowy zasobu.
- **VPN** – *Virtual Private Network* – szyfrowane, prywatne połączenie z siecią.
- **Wi-Fi** – standard bezprzewodowej łączności sieciowej.
- **BIOS/UEFI** – oprogramowanie układowe płyty głównej odpowiedzialne za start komputera i konfigurację sprzętu.
- **M365** – Microsoft 365 – usługi/aplikacje Microsoft (konto użytkownika, chmura itp.).
- **Service Tag** – numer identyfikacyjny urządzenia (zwł. Dell) używany do wsparcia/serwisu.
- **Opt-in** – świadome włączenie funkcji przez użytkownika (domyślnie wyłączone do czasu wyrażenia zgody).