



Digital sovereignty po polsku, czyli co polskie MŚP wiedzą i myślą o suwerenności cyfrowej

Raport home.pl, październik 2025 r.

Spis treści

Raport w pigułce	3
Wprowadzenie	4
Znaczenie suwerenności cyfrowej	5
Wybór dostawcy usług IT a suwerenność cyfrowa	6
Podsumowanie	11

Raport w pigułce

Oto, czego dowiesz się z opracowania „Digital sovereignty po polsku, czyli co polskie MŚP wiedzą i myślą o suwerenności cyfrowej”.



Polscy przedsiębiorcy formułują względem dostawców IT najwyższe oczekiwania w zakresie przestrzegania standardów i norm (np. standardów bezpieczeństwa, certyfikatów). **Aż 90% polskich MŚP oczekuje od dostawców IT ścisłego przestrzegania zasad.** To najwyższy wynik wśród ankietowanych krajów i najważniejszy poruszony w badaniu aspekt suwerenności cyfrowej, na który zwracają uwagę polscy przedsiębiorcy.



Stabilność infrastruktury oraz bezpieczna lokalizacja danych to dla polskich firm priorytet przy wyborze dostawcy IT — **88% respondentów wskazuje ten aspekt jako kluczowy.**



86% polskich firm uważa, że stosowana technologia powinna być niezależna od decyzji politycznych podejmowanych poza Unią Europejską — to jeden z najwyższych wyników wśród badanych krajów.



Dla 83% polskich MŚP ochrona danych przed możliwością dostępu organów spoza UE ma kluczowe znaczenie. Świadomość ta dowodzi, że firmy zaczynają traktować lokalizację danych nie tylko jako kwestię techniczną, ale też jako element związany z bezpieczeństwem prawnym i geopolitycznym.



Bezpieczeństwo danych i stabilność usług ważniejsze niż odporność łańcucha dostaw. 1 na 5 polskich firm (21%) uważa za mało ważne, czy wybrany dostawca usług IT jest niezależny od poszczególnych dostawców i nieprzerwanie dysponuje wymaganymi komponentami sprzętowymi IT.

Wprowadzenie

W świecie, w którym dane są nową walutą, a dostęp do technologii decyduje o pozycji konkurencyjnej, pytanie o to, kto faktycznie kontroluje cyfrową infrastrukturę, nie jest już teoretyczne — to kwestia bezpieczeństwa i przyszłości biznesu. Pojęcie suwerenności cyfrowej (z angielskiego digital sovereignty), które wciąż jeszcze w Polsce traktowane jako niszowe, w Europie coraz częściej pojawia się w strategicznych rozmowach o przyszłości firm. Oznacza ono realną zdolność przedsiębiorstw do samodzielnego decydowania o tym, gdzie i jak przechowywane są ich dane, jakim standardom bezpieczeństwa podlegają oraz czy technologie, z których korzystają, pozostają zależne wyłącznie od lokalnej i europejskiej jurysdykcji.

W kontekście rosnących napięć geopolitycznych — od wojny w Ukrainie, przez zmieniającą się sytuację na Bliskim Wschodzie, po globalne regulacje dotyczące transferu danych — **suwerenność cyfrowa staje się fundamentem stabilności biznesu**. W wymiarze egzekucyjnym oznacza to konieczność świadomego wyboru partnerów technologicznych i rozwiązań, które zapewnią im niezależność w długim horyzoncie czasowym.

Jako cyfrowy partner polskich przedsiębiorstw, home.pl wspiera je — zwłaszcza sektor MŚP — w przechodzeniu przez proces digitalizacji w sposób świadomy, bezpieczny i suwerenny. Nasza misja to nie tylko dostarczanie nowoczesnych rozwiązań IT, ale także edukowanie przedsiębiorców i wskazywanie kierunków, w których powinni podążać z myślą o stabilnej i bezpiecznej cyfrowej przyszłości.

Zachęcamy do zapoznania się z wynikami badania, które dzięki członkostwu home.pl w grupie IONOS obejmuje także dane z 6 krajów Europy: Niemiec, Wielkiej Brytanii, Hiszpanii, Francji, Holandii i Szwecji. W tym kontekście opracowanie pozwala na analizę zjawiska w porównaniu z sześcioma innymi państwami o różnym stopniu rozwoju gospodarczego i PKB oraz z występującymi różnicami w kontekście społecznym i kulturowym.

Głęboko wierzymy, że opracowanie będzie okazją do refleksji na temat suwerenności cyfrowej, a w dłuższej perspektywie zapewni jej wiodące miejsce w strategiach biznesowych polskich firm.

Zapraszamy do lektury.

1. Znaczenie suwerenności cyfrowej

W kontekście globalnych wydarzeń politycznych (np. prezydentura w USA, konflikt na Bliskim Wschodzie, wojna w Ukrainie) wybierając dostawców usług technologicznych (np. dostawców hostingu/chmury), jak ważne jest dla Ciebie, aby gwarantowali Ci kontrolę nad Twoimi danymi (tzw. „suwerenność cyfrową”)?

Francja		18%	73%
Hiszpania		12%	83%
Holandia		16%	79%
Niemcy		12%	82%
Polska		22%	73%
Szwecja		13%	78%
Wielka Brytania		7%	82%



■ Mało ważne i nieważne ■ Ważne i bardzo ważne

W Polsce 73% przedstawicieli sektora MŚP uznaje suwerenność cyfrową za ważną lub bardzo ważną, co jest wynikiem zbliżonym do średniej europejskiej. Z jednej strony, pokazuje to, że polskie firmy są coraz bardziej świadome strategicznego znaczenia kontroli nad swoimi danymi i infrastrukturą w kontekście globalnych zawirowań. Z drugiej strony, fakt, że wynik ten jest niższy niż w krajach takich jak Hiszpania (83%), Niemcy (82%) czy Wielka Brytania (82%), sugeruje, że **polscy przedsiębiorcy, choć dostrzegają problem, rzadziej przekładają tę świadomość na konkretne procedury i decyzje zakupowe**. Może to wynikać z mniejszego doświadczenia z negatywnymi konsekwencjami braku suwerenności lub z mniejszej presji regulacyjnej i rynkowej.

2. Wybór dostawcy usług IT a suwerenność cyfrowa

Jak ważne są dla Ciebie następujące aspekty przy wyborze dostawców usług IT (np. dostawców hostingu/chmury) w odniesieniu do kontroli nad Twoimi danymi (tzw. „suwerenność cyfrowa”)?

2.1 Mogę samodzielnie decydować, kto ma dostęp do moich danych i może je zmieniać (np. dokumenty, dane klientów)

	Francja	Hiszpania	Holandia	Niemcy	Polska	Szwecja	Wielka Brytania
Mało ważne i nieważne	8%	10%	8%	8%	14%	10%	3%
Ważne i bardzo ważne	87%	87%	88%	89%	82%	81%	87%

82% polskich MŚP wskazuje, że ważny i bardzo ważny, przy wyborze dostawcy usług IT, jest dla nich aspekt samodzielnego decydowania o dostępie do swoich danych. **Wynik ten pokazuje wyraźne oczekiwania wobec przejrzystości i zarządzania uprawnieniami, choć jednocześnie plasuje Polskę poniżej średniej dla krajów takich jak Niemcy (89%) czy Holandia (88%).** Różnica ta może wynikać z dwóch przyczyn. Po pierwsze, polskie firmy mogły rzadziej doświadczać naruszeń danych lub sytuacji, w których utrata kontroli miała poważne konsekwencje, dlatego ich podejście do tego aspektu może być mniej rygorystyczne. Po drugie, może to również świadczyć o większym zaufaniu lub mniejszej wnikliwości w ocenianiu warunków dostawców zewnętrznych, co otwiera pole do dalszej edukacji w zakresie zarządzania uprawnieniami i transparentności usług.



2.2 Ochrona danych osobowych i tajemnic handlowych przed dostępem organów zagranicznych

	Francja	Hiszpania	Holandia	Niemcy	Polska	Szwecja	Wielka Brytania
Mało ważne i nieważne	11%	8%	7%	9%	15%	9%	6%
Ważne i bardzo ważne	83%	87%	86%	87%	83%	84%	83%

Dla 83% polskich MŚP — tak samo jak dla ich odpowiedników w Wielkiej Brytanii i we Francji — ochrona danych przed możliwością dostępu organów spoza UE ma kluczowe znaczenie.

Ten wysoki wynik świadczy o rosnącej świadomości geopolitycznych i regulacyjnych ryzyk związanych z przechowywaniem danych. Polscy przedsiębiorcy zaczynają rozumieć, że lokalizacja serwerów to nie tylko kwestia techniczna, ale też zabezpieczenie prawne, chroniące firmę przed ingerencjami obcych jurysdykcji. Ten aspekt staje się priorytetem, co może być efektem nagłośnienia spraw związanych z przepisami takimi jak U.S. CLOUD Act.

2.3 Zastosowana technologia funkcjonuje niezależnie od pozaeuropejskich decyzji politycznych

	Francja	Hiszpania	Holandia	Niemcy	Polska	Szwecja	Wielka Brytania
Mało ważne i nieważne	14%	12%	16%	11%	7%	14%	14%
Ważne i bardzo ważne	76%	81%	76%	84%	86%	75%	63%

Polska wyróżnia się na tle badanych europejskich krajów, przywiązując najwyższą wagę do niezależności technologicznej od pozaeuropejskich decyzji politycznych (86%). Tak wysoki wynik (dla porównania, w Wielkiej Brytanii wynosi 63%) może być bezpośrednio powiązany z bliskością konfliktu zbrojnego w Ukrainie. Sytuacja geopolityczna sprawiła, że polskie firmy są szczególnie wyczulone na ryzyka związane z globalnymi napięciami i potencjalnymi sankcjami technologicznymi. W efekcie nie postrzegają suwerenności cyfrowej jako abstrakcyjnego konceptu, ale traktują ją jako realne zabezpieczenie stabilności swojego biznesu.



Przez blisko 30 lat home.pl towarzyszy polskim firmom, szczególnie MŚP, w ich cyfrowej transformacji. Zaczynaliśmy od dostarczania podstawowych usług, a dziś nasza rola ewoluuje. Stajemy się cyfrowym przewodnikiem, który nie tylko wspiera biznes, ale także dba o jego bezpieczeństwo i suwerenność. Wierzymy, że w dzisiejszym świecie, gdzie dane są najcenniejszym kapitałem, lokalny partner, który rozumie polskie realia i chroni cyfrowe aktywa, to klucz do sukcesu.

Nasze doświadczenie, poparte kompleksowym zestawem certyfikatów, a także infrastruktura podlegająca wyłącznie lokalnej i europejskiej jurysdykcji daje przedsiębiorcom pewność, że ich cyfrowa przyszłość jest w dobrych rękach.

Magdalena Chudzikiewicz, General Manager w firmie home.pl

2.4 Przestrzeganie określonych standardów i zasad

	Francja	Hiszpania	Holandia	Niemcy	Polska	Szwecja	Wielka Brytania
Mało ważne i nieważne	9%	7%	10%	7%	4%	11%	4%
Ważne i bardzo ważne	84%	86%	83%	88%	90%	78%	83%

90% pozytywnych odpowiedzi na pytanie o wagę zgodności ze standardami i zasadami plasuje Polskę na pozycji lidera wśród badanych europejskich krajów. Wysoki wynik pokazuje, że polski biznes ma najwyższe oczekiwania co do jakości i przejrzystości usług IT. Takie podejście świadczy o dojrzewaniu rynku i rosnącej świadomości na temat certyfikatów i norm, takich jak ISO, które są namacalnym dowodem na wiarygodność i profesjonalizm dostawcy. To z kolei rzutuje na decyzje zakupowe, które polscy przedsiębiorcy podejmują coraz częściej w oparciu o wspomniane obiektywne wskaźniki jakości i bezpieczeństwa.





Badania pokazują, że polskie firmy są liderami w Europie pod względem przywiązywania wagi do zgodności ze standardami i zasadami w obszarze IT. W home.pl w pełni rozumiemy tę potrzebę i od lat budujemy naszą wiarygodność, inwestując w najwyższe standardy.

Uwiarygodnieniem naszej dbałości o cyfrową suwerenność jest najszerzy na rynku pakiet certyfikatów, który obejmuje ISO 9001, ISO 27001 oraz, co kluczowe, niedawno uzyskany ISO 22301, poświadczający naszą zdolność do zapewnienia ciągłości działania w każdych warunkach. Te certyfikaty to dla naszych klientów namacalny dowód, że home.pl jest partnerem godnym zaufania, gotowym sprostać zarówno ich oczekiwaniom biznesowym, jak i rosnącym wymogom regulacyjnym, takim jak DORA czy NIS2.

Grzegorz Bielecki, Chief Information Security Officer w home.pl

2.5 Wybrany dostawca gwarantuje bezpieczną lokalizację infrastruktury i zapewnia stabilne połączenie z internetem

	Francja	Hiszpania	Holandia	Niemcy	Polska	Szwecja	Wielka Brytania
Mało ważne i nieważne	11%	8%	8%	8%	10%	12%	4%
Ważne i bardzo ważne	84%	88%	86%	88%	88%	81%	87%

Stabilność infrastruktury oraz bezpieczna lokalizacja danych to dla polskich firm priorytet przy wyborze dostawcy IT – 88% respondentów wskazuje ten aspekt jako kluczowy, plasując Polskę w ścisłej czołówce zestawienia, na równi z Niemcami. Ten wysoki wynik świadczy o pragmatycznym podejściu polskich przedsiębiorców, którzy rozumieją, że ciągłość działania i minimalizacja ryzyka operacyjnego, takiego jak awarie czy przerwy w dostępie, są kluczowe dla ich codziennego funkcjonowania. Preferencja dla lokalnej, sprawdzonej infrastruktury wynika zapewne również z chęci uniknięcia nieprzewidzianych zakłóceń, które mogłyby sparaliżować biznes. **To dowód, że praktyczne aspekty bezpieczeństwa stają się równie ważne, co kwestie regulacyjne.**





Suwerenność cyfrowa to w home.pl nie tylko idea, lecz fundament operacyjny. Osiągamy ją dzięki konsekwentnemu wdrażaniu strategii opartej na lokalizacji i dywersyfikacji. Wszystkie nasze centra danych znajdują się w Polsce, co zapewnia pełną kontrolę nad infrastrukturą i danymi. Dążymy do maksymalnej niezależności, stosując podejście dywersyfikacji i multivendoringu – uniezależniając się od jednego dostawcy usług internetowych, sprzętu czy rozwiązań. Dodatkowo, tam, gdzie to możliwe, współpracujemy priorytetowo z polskimi i europejskimi dostawcami.

Wysoki poziom cyberbezpieczeństwa, w tym ochrona przed atakami DDoS, to nasz priorytet, który gwarantuje, że dane naszych klientów pozostają bezpieczne, a ich biznes działa bez zakłóceń.

Dariusz Grajnert, Dyrektor Działu IT w firmie home.pl

2.6 Wybrany dostawca usług IT jest niezależny od poszczególnych dostawców i nieprzerwanie dysponuje wymaganymi komponentami sprzętowymi IT

	Francja	Hiszpania	Holandia	Niemcy	Polska	Szwecja	Wielka Brytania
Mało ważne i nieważne	18%	14%	12%	11%	21%	16%	9%
Ważne i bardzo ważne	73%	81%	81%	83%	75%	75%	74%

75% polskich przedsiębiorców uznaje niezależność sprzętową dostawców IT za ważną. To wynik nieco niższy niż średnia w badaniu (77%) i znacznie niższy od liderów zestawienia – Niemiec (83%) czy Holandii (81%). Może to dowodzić, że polskie firmy nadal koncentrują się głównie na bezpieczeństwie danych i stabilności usług, a w mniejszym stopniu na odporności łańcucha dostaw sprzętu. Brak dostatecznej uwagi dla tego aspektu zwiększa ryzyko uzależnienia się od pojedynczych producentów i podatności na globalne kryzysy komponentowe.

To podejście, choć być może tańsze w krótkim terminie, może zwiększać ryzyko uzależnienia od pojedynczych producentów i wrażliwości na globalne kryzysy w łańcuchach dostaw. Wskazuje to na potrzebę dalszej edukacji w zakresie strategii multivendorowych.

Podsumowanie

Zaprezentowane w raporcie wyniki badania na temat stanu wiedzy polskich i europejskich MŚP w zakresie suwerenności cyfrowej prowadzą do wniosku, że ich specyfika oraz wiodące różnice wynikają z kilku czynników, spośród których najważniejsze to tło geopolityczne oraz różnice w dojrzałości rynku i doświadczeniach przedsiębiorców.

Polscy przedsiębiorcy, w porównaniu do swoich odpowiedników w krajach Europy Zachodniej, są bardziej wrażliwi na ryzyka związane z niestabilnością polityczną. Położenie geopolityczne Polski i bliskość konfliktu w Ukrainie sprawia, że postrzegają oni suwerenność cyfrową nie jako abstrakcyjne zjawisko, lecz jako realne zabezpieczenie biznesu przed zewnętrznymi naciskami. Dlatego też w badaniu największy odsetek polskich firm (86%) uważa, że technologia powinna funkcjonować niezależnie od pozaeuropejskich decyzji politycznych, znacznie wyprzedzając pod tym względem inne badane kraje.

Na różnice w wynikach między Polską a pozostałymi badanymi krajami europejskimi może wpływać również kwestia dojrzałości rynku i kwestia doświadczenia w obcowaniu ze zjawiskiem suwerenności cyfrowej. Mimo dużej świadomości geopolitycznej, polski rynek MŚP wciąż jest na etapie, w którym deklaracje nie zawsze przekładają się na konkretne działania. Niższy wynik w kategorii ogólnej wagi suwerenności cyfrowej (73% vs. 83% w Hiszpanii) oraz w kwestii niezależności sprzętowej (75% vs. 83% w Niemczech) może świadczyć o tym, że polskie firmy rzadziej doświadczają negatywnych konsekwencji braku kontroli nad danymi lub uzależnienia od jednego dostawcy. Ten brak dotkliwych doświadczeń może prowadzić do mniejszego rygoryzmu w procesach decyzyjnych dotyczących wyboru partnerów technologicznych.

Jednocześnie polskie firmy są liderami wśród badanych europejskich krajów pod względem wymagań dotyczących zgodności ze standardami i zasadami (90%). Może to wynikać z ogólnej tendencji na polskim rynku do poszukiwania wiarygodności i potwierdzenia jakości usług poprzez obiektywne certyfikaty, takie jak ISO. W dobie rosnącej liczby dostawców IT, posiadane przez nich certyfikaty stanowią dla polskich firm rzetelne i namacalne potwierdzenie jakości i profesjonalizmu, co zdecydowanie ułatwia proces weryfikacji i wyboru partnera.