

POLITYKA PRYWATNOŚCI DATAMINDER

Wersja: DM-PP-310826-PL | obowiązuje od: 31.08.2026

1. Najważniejsze informacje

Niniejsza Polityka wyjaśnia, w jaki sposób DataMinder sp. z o.o. przetwarza dane osobowe osób odwiedzających serwisy DataMinder, zakładających konto, korzystających z aplikacji, dokonujących płatności, kontaktujących się z nami, zapisujących się na newsletter lub listę oczekujących, uczestniczących w testach lub nagrywanych spotkaniach oraz korzystających z profili DataMinder w mediach społecznościowych.

Zagadnienie	Najważniejsza informacja
Administrator	DataMinder sp. z o.o., ul. Lipnowska 207, 09-400 Maszewo Duże.
Kontakt	contact@dataminder.ai
Główne cele	Świadczenie usługi, konto i bezpieczeństwo, płatności, kontakt i wsparcie, AI, nagrywanie spotkań, analityka oraz marketing – zgodnie z wyborem użytkownika.
Dane klientów	Dla danych osobowych w datasetach klienta DataMinder co do zasady działa jako podmiot przetwarzający, a klient jako administrator.
Prawa	Dostęp, sprostowanie, usunięcie, ograniczenie, przenoszenie, sprzeciw, wycofanie zgody i skarga do Prezesa UODO – zależnie od podstawy i okoliczności.

2. Administrator i kontakt

Administratorem danych osobowych przetwarzanych dla własnych celów DataMinder jest DataMinder sp. z o.o. z siedzibą przy ul. Lipnowskiej 207, 09-400 Maszewo Duże, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy w Łodzi, XX Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0001152130, NIP 7743295226, REGON 540761152 („DataMinder”, „my”).

W sprawach dotyczących prywatności, realizacji praw lub bezpieczeństwa danych skontaktuj się z nami pod adresem contact@dataminder.ai. Możemy poprosić o informacje niezbędne do potwierdzenia tożsamości, jeżeli jest to potrzebne do bezpiecznej obsługi żądania.

3. Zakres Polityki i role DataMinder

3.1. DataMinder jako administrator

Jesteśmy administratorem danych, gdy samodzielnie ustalamy cele i sposoby przetwarzania, w szczególności dla danych konta, uwierzytelniania, płatności i kredytów, bezpieczeństwa i diagnostyki, kontaktu i wsparcia, komunikacji usługowej, newslettera, analityki, marketingu, rekrutacji testerów, nagrywania i transkrypcji spotkań oraz obsługi praw i roszczeń.

3.2. DataMinder jako podmiot przetwarzający

Jeżeli klient przesyła do DataMinder dataset zawierający dane osobowe innych osób i określa cel analizy, klient pozostaje administratorem tych danych, a DataMinder co do zasady przetwarza je jako podmiot przetwarzający, na udokumentowane polecenie klienta. Zasady takiego przetwarzania określa umowa powierzenia danych. Osoby, których dane znajdują się w datasecie klienta, powinny w pierwszej kolejności kontaktować się z tym klientem.

Możemy jednak działać jako administrator dla niektórych odrębnych informacji powstających przy świadczeniu usługi, np. danych rozliczeniowych, bezpieczeństwa, logów wymaganych do ochrony systemu lub danych potrzebnych do dochodzenia roszczeń. Rola jest oceniana osobno dla każdego celu.

4. Jakie dane przetwarzamy

Kategoria	Przykładowe dane
Konto i identyfikacja	Imię, nazwisko, adres e-mail, identyfikator konta, ustawienia, dane uwierzytelniające lub token Google OAuth.
Projekty i analizy	Pliki, datasety, schematy, nazwy pól, próbki wartości, hipotezy, konfiguracje analiz, wyniki, wykresy, raporty i notatniki.
Funkcje AI	Polecenia i wiadomości, historia rozmowy, załączniki, statystyki datasetu, wyniki analiz, odpowiedzi, raporty, błędy i metadane wykonania.
Płatności i rozliczenia	Dane klienta i transakcji, kraj lub region, status płatności, identyfikatory Stripe; dane karty są podawane bezpośrednio Stripe.
Kontakt i wsparcie	Dane kontaktowe, treść korespondencji i załączników, informacje o koncie, projekcie, urządzeniu, przeglądarce i błędach.
Dane techniczne i bezpieczeństwo	Adres IP, znaczniki czasu, identyfikatory sesji, urządzenia i żądania, logi, dane diagnostyczne oraz informacje o nietypowej aktywności.
Analityka i marketing	Identyfikatory online, dane o urządzeniu i przeglądarce, przybliżona lokalizacja, odsłony, kliknięcia, nawigacja, interakcje i konwersje – po uzyskaniu wymaganej zgody.
Media społecznościowe	Nazwa profilu, publiczne dane profilu, reakcje, komentarze i wiadomości kierowane do profili DataMinder.

Kategoria	Przykładowe dane
Nagrania spotkań	Głos, ewentualnie wizerunek, treść wypowiedzi, transkrypcja, notatki, podsumowanie i metadane – po uzyskaniu właściwej zgody.

Zakres danych zależy od sposobu korzystania z usługi oraz treści przekazanych przez użytkownika. Przed przesłaniem datasetu użytkownik musi usunąć dane zbędne, bezpośrednie identyfikatory oraz informacje pozwalające DataMinder jednoznacznie zidentyfikować osobę. Jeżeli dane są pseudonimizowane, klucz pozwalający na ponowną identyfikację musi pozostać oddzielnie u użytkownika i nie może być przekazany DataMinder. Dane szczególnych kategorii, dane dotyczące wyroków skazujących i naruszeń prawa oraz dane dzieci mogą być przetwarzane wyłącznie po minimalizacji i co najmniej pseudonimizacji, bez przekazania klucza identyfikacyjnego, jeżeli użytkownik posiada właściwą podstawę prawną i zastosował zabezpieczenia adekwatne do ryzyka. Dane prawidłowo zanonimizowane nie są danymi osobowymi; pseudonimizowane nadal podlegają RODO.

5. Cele i podstawy prawne

Cele, podstawy prawne, zakres danych, kryteria retencji i źródła zostały opisane szczegółowo w Załączniku nr 2 – Cele przetwarzania danych osobowych, stanowiącym część niniejszej Polityki. W skrócie:

Cel	Podstawa prawna
Konto, uwierzytelnianie, projekty, analizy, kredyty i komunikacja usługowa	Art. 6 ust. 1 lit. b RODO – zawarcie i wykonanie umowy.
Płatności, księgowość, podatki, reklamacje i prawa osób	Art. 6 ust. 1 lit. b lub c RODO – umowa i obowiązki prawne; w odpowiednim zakresie także art. 6 ust. 1 lit. f RODO.
Bezpieczeństwo, diagnostyka, zapobieganie nadużyciom, wsparcie i roszczenia	Art. 6 ust. 1 lit. f RODO – prawnie uzasadnione interesy DataMinder lub użytkowników; obowiązki bezpieczeństwa także art. 6 ust. 1 lit. c RODO.
Newsletter, lista oczekujących, nagrywanie spotkań, analityka i reklama	Art. 6 ust. 1 lit. a RODO – zgoda; dla komunikacji i technologii końcowych także art. 398–399 Prawa komunikacji elektronicznej.
Dane w datasetach klienta	Art. 28 RODO i udokumentowane polecenia klienta; podstawę z art. 6 i – jeżeli dotyczy – art. 9 RODO ustala klient będący administratorem.

Jeżeli opieramy się na prawnie uzasadnionym interesie, oceniamy niezbędność przetwarzania i wpływ na prawa osoby. Możesz wnieść sprzeciw z przyczyn związanych z Twoją szczególną sytuacją; w przypadku marketingu bezpośredniego sprzeciw jest bezwarunkowy.

6. Czy podanie danych jest obowiązkowe

Podanie danych wymaganych podczas rejestracji, płatności lub realizacji określonej funkcji jest dobrowolne, lecz konieczne do zawarcia lub wykonania umowy albo wykonania żądanej czynności. Bez danych oznaczonych jako wymagane nie będziemy mogli utworzyć konta, zrealizować płatności, przeprowadzić analizy lub odpowiedzieć na zgłoszenie.

Podanie danych na potrzeby newslettera, listy oczekujących, analityki, reklamy lub nagrywania spotkania jest dobrowolne. Odmowa albo wycofanie zgody nie wpływa na możliwość korzystania z podstawowych funkcji usługi, które nie wymagają takiej zgody.

7. Skąd pozyskujemy dane

- bezpośrednio od Ciebie – podczas rejestracji, korzystania z usługi, płatności, kontaktu, zapisu na newsletter lub udziału w spotkaniu;
- od klienta lub osoby działającej w jego imieniu – gdy dane znajdują się w przekazanym datasetcie;
- automatycznie z urządzenia, przeglądarki, aplikacji i infrastruktury – w zakresie danych technicznych, bezpieczeństwa i aktywności;
- od dostawców logowania, płatności, komunikacji, nagrywania i transkrypcji spotkań, analityki, reklamy i mediów społecznościowych – w zakresie wynikającym z użytej funkcji i ustawień;
- z wyników działania DataMinder – np. wygenerowanych analiz, raportów, odpowiedzi AI i danych rozliczających wykorzystanie.

8. Odbiorcy danych i narzędzia zewnętrzne

Możemy ujawniać dane podmiotom wspierającym działanie DataMinder, wyłącznie w zakresie niezbędnym do danego celu. Należą do nich dostawcy infrastruktury chmurowej, systemów AI, poczty i uwierzytelniania, płatności, hostingu treści, nagrywania i transkrypcji spotkań, analityki, badania użyteczności, reklamy oraz serwisów społecznościowych.

Publiczna lista używanych narzędzi, podmiotów umownych, celów wykorzystania oraz dokumentów dostawców znajduje się w Załączniku nr 1 – Wykaz narzędzi zewnętrznych. Lista obejmuje m.in. AWS, Microsoft Foundry / Azure OpenAI, Google Workspace i Google OAuth, Google Analytics 4, Stripe, Sanity, Hotjar, Meta Pixel, Fireflies.ai oraz profile DataMinder w LinkedIn, Facebook i Instagram.

Dane mogą być również udostępniane upoważnionym pracownikom i współpracownikom, doradcom prawnym i księgowym, bankom, operatorom płatności oraz organom publicznym, jeżeli wynika to z prawa lub jest konieczne do ustalenia, dochodzenia lub obrony roszczeń.

9. Przekazywanie danych poza Europejski Obszar Gospodarczy

W związku z korzystaniem przez Administratora z usług niektórych dostawców, w szczególności AWS, Google, Meta, LinkedIn, Sanity, Hotjar, Stripe, Microsoft oraz Fireflies.ai, dane osobowe mogą być przekazywane do państw spoza Europejskiego Obszaru Gospodarczego lub mogą być z takich państw dostępne. Fireflies.ai domyślnie przechowuje i przetwarza dane w Stanach Zjednoczonych.

Przekazywanie odbywa się na podstawie odpowiedniego mechanizmu przewidzianego w rozdziale V RODO, w szczególności decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony, EU–US Data Privacy Framework dla objętego nim certyfikowanego podmiotu albo standardowych klauzul umownych, wraz z dodatkowymi zabezpieczeniami, gdy są wymagane.

Mechanizmy wskazane przez dostawców obejmują w szczególności: EU–US Data Privacy Framework dla objętych nim certyfikowanych podmiotów w Stanach Zjednoczonych oraz standardowe klauzule umowne zatwierdzone decyzją wykonawczą Komisji (UE) 2021/914, stosowane, gdy transfer nie jest objęty decyzją stwierdzającą odpowiedni stopień ochrony. Szczegółowe dokumenty i warunki transferowe właściwe dla poszczególnych narzędzi wskazano w Załączniku nr 1. Na żądanie udostępnimy informację o stosowanych zabezpieczeniach lub wskażemy miejsce, w którym można uzyskać ich kopię

10. Okres przechowywania danych

Dane konta, projektów, notebooków, datasetów i raportów pozostają w aktywnym koncie bez z góry określonego terminu, do chwili ich usunięcia przez użytkownika, usunięcia konta albo zakończenia umowy wymagającego usunięcia. Usunięcie projektu powoduje usunięcie informacji i wyników związanych z projektem, ale nie usuwa datasetu lub pliku źródłowego przechowywanego niezależnie w koncie; taki dataset lub plik jest usuwany na odrębne polecenie użytkownika albo wraz z kontem. Usunięcie konta uruchamia usunięcie wszystkich związanych z nim danych i artefaktów z aktywnych systemów, cache, kolejek i kopii dostawców w terminie do 30 dni. Automatyczne kopie zapasowe RDS są usuwane przez nadpisanie w cyklu retencji nieprzekraczającym 35 dni, a logi i ślady LLM – nie później niż w terminie 90 dni. Do czasu usunięcia kopie zapasowe są odizolowane od zwykłego przetwarzania i mogą zostać użyte wyłącznie do odtworzenia systemu lub zapewnienia bezpieczeństwa. Dane wymagane przez prawo albo niezbędne do ustalenia, dochodzenia lub obrony roszczeń mogą być przechowywane dłużej, wyłącznie w niezbędnym zakresie. Nagrania, transkrypcje, podsumowania i notatki ze spotkań w Fireflies.ai przechowujemy przez 3 miesiące od dnia spotkania, z możliwością wcześniejszego usunięcia po wycofaniu zgody, jeżeli nie istnieje inna podstawa dalszego przechowywania.

Dane	Obecnie przyjęta informacja
Logi ECS CloudWatch	30 dni.
Dokumentacja księgowa	Co do zasady 5 lat zgodnie z art. 74 ustawy o rachunkowości.
Dokumenty podatkowe	Do upływu terminu przedawnienia zobowiązania podatkowego, co do zasady 5 lat od końca roku, w którym upłynął termin płatności.
Dane przetwarzane na podstawie zgody	Do wycofania zgody albo zakończenia celu; dowód zgody może być przechowywany przez okres potrzebny do wykazania zgodności i obrony przed roszczeniami.
Logi Lambda i bazy danych	1 miesiąc.
Ślady LLM w self-hosted Langfuse	90 dni; po usunięciu konta stanowią najpóźniejszą granicę usunięcia logów i śladów powiązanych z kontem.

Dane	Obecnie przyjęta informacja
Pozostałe dane	Szczegółowe kryteria zawiera Załącznik nr 2.
Nagrania, transkrypcje i notatki ze spotkań	3 miesiące od dnia spotkania; wcześniej po wycofaniu zgody, jeżeli brak innej podstawy dalszego przechowywania.

11. Pliki cookies, pamięć urządzenia, analityka i marketing

11.1. Technologie niezbędne i preferencje

DataMinder korzysta z technologii koniecznych do uwierzytelniania, bezpieczeństwa i zapamiętania decyzji dotyczącej prywatności. Zidentyfikowane technologie własne obejmują cookie służące do uwierzytelniania (30 dni), służące do ustawienia interfejsu (7 dni), służące do zapamiętania języka (1 rok) oraz lokalną pamięć dla wyboru zgody i zakładki. Niektóre wpisy lokalnej pamięci nie mają technicznie ustawionego terminu wygaśnięcia.

11.2. Analityka, badanie użyteczności i reklama

Po uzyskaniu odpowiedniej zgody użytkownika korzystamy z Google Analytics 4 do pomiaru korzystania z serwisu, z Hotjar do badania użyteczności oraz z Meta Pixel do pomiaru kampanii, konwersji i reklam. Przed udzieleniem zgody, po jej odmowie oraz po jej wycofaniu narzędzia te pozostają wyłączone i nie zbierają danych. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem. Informacje o dostawcach znajdują się w Załączniku nr 1.

Podstawą przetwarzania danych osobowych jest zgoda z art. 6 ust. 1 lit. a RODO, a podstawą przechowywania informacji lub dostępu do informacji w urządzeniu końcowym – zgoda wymagana przez art. 399 Prawa komunikacji elektronicznej. Zgodę można wycofać bez wpływu na zgodność wcześniejszego przetwarzania.

12. Newsletter i komunikacja marketingowa

Newsletter i inne wiadomości marketingowe wysyłamy na podstawie dobrowolnej zgody z art. 6 ust. 1 lit. a RODO oraz zgody wymaganej przez art. 398 Prawa komunikacji elektronicznej. Możesz zrezygnować w dowolnym czasie, korzystając z mechanizmu dostępnego w wiadomości lub pisząc na contact@dataminder.ai.

Po rezygnacji możemy zachować minimalną informację na liście blokującej, aby respektować Twój wybór, oraz dowód zgody i jej wycofania przez okres potrzebny do wykazania zgodności i obrony przed roszczeniami.

13. Nagrywanie, transkrypcja i notatki ze spotkań

Po uzyskaniu wymaganej zgody uczestników możemy korzystać z Fireflies.ai do nagrywania spotkania, sporządzenia transkrypcji, podsumowania i notatek. Zakres danych może obejmować

imiona i nazwiska lub identyfikatory uczestników, adresy e-mail, dane kalendarza, głos, ewentualnie wizerunek, treść wypowiedzi i metadane spotkania. Odmowa nagrania nie ogranicza dostępu do podstawowych funkcji DataMinder.

Materiały ze spotkania przechowujemy przez 3 miesiące. Jeżeli spotkanie obejmuje Dane Powierzone przez klienta, DataMinder przetwarza je na udokumentowane polecenie klienta, a Fireflies.ai działa jako podprocesor. Fireflies.ai domyślnie przechowuje i przetwarza dane w Stanach Zjednoczonych; informacje o mechanizmach transferowych i dokumentach dostawcy znajdują się w Załączniku nr 1.

14. Sztuczna inteligencja i zautomatyzowane decyzje

DataMinder wykorzystuje Microsoft Foundry / Azure OpenAI do generatywnych funkcji wspierających formułowanie hipotez, wyjaśnianie i prezentację wyników oraz tworzenie raportów i treści pomocniczych. Obliczenia statystyczne są wykonywane przez odrębny, deterministyczny komponent. Szczegóły zawiera Załącznik nr 3 – Informacja o wykorzystaniu sztucznej inteligencji.

Użytkownik jest informowany o interakcji z funkcją AI. Wyniki AI mają charakter pomocniczy, mogą zawierać błędy i powinny zostać zweryfikowane. Zgodnie z obecnym opisem usługi DataMinder nie podejmuje wobec użytkowników decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, które wywołują skutki prawne lub podobnie istotnie na nich wpływają w rozumieniu art. 22 RODO.

15. Bezpieczeństwo danych

Stosujemy środki techniczne i organizacyjne dobrane do charakteru danych i ryzyka, obejmujące kontrolę dostępu, szyfrowanie transmisji, rozwiązania infrastrukturalne, kopie zapasowe, logowanie zdarzeń oraz ograniczenie dostępu personelu. Regularnie oceniamy potrzebę aktualizacji zabezpieczeń.

Żadna metoda transmisji ani przechowywania nie gwarantuje całkowitego bezpieczeństwa. Jeżeli podejrzewasz naruszenie lub nieuprawniony dostęp do konta, niezwłocznie skontaktuj się z nami pod adresem contact@dataminder.ai.

16. Prawa osób

W zależności od podstawy przetwarzania i okoliczności przysługują Ci następujące prawa:

- dostęp do danych i otrzymanie ich kopii;
- sprostowanie nieprawidłowych lub uzupełnienie niekompletnych danych;
- usunięcie danych;
- ograniczenie przetwarzania;
- przenoszenie danych, gdy przetwarzanie odbywa się na podstawie zgody lub umowy w sposób zautomatyzowany;
- sprzeciw wobec przetwarzania opartego na prawnie uzasadnionym interesie, w tym bezwarunkowy sprzeciw wobec marketingu bezpośredniego;
- wycofanie zgody w dowolnym czasie, bez wpływu na zgodność przetwarzania dokonanego przed jej wycofaniem;

- niepodleganie decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu w przypadkach określonych w art. 22 RODO.

Aby skorzystać z prawa, napisz na contact@dataminder.ai. Odpowiemy bez zbędnej zwłoki, co do zasady w ciągu miesiąca. Termin może zostać przedłużony o kolejne dwa miesiące ze względu na złożony charakter lub liczbę żądań; poinformujemy o przedłużeniu i jego przyczynach.

Masz również prawo wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych. Aktualne informacje o sposobie złożenia skargi są dostępne na stronie <https://uodo.gov.pl>.

17. Dane dzieci

Usługa DataMinder nie jest przeznaczona dla osób niepełnoletnich i konta takich osób nie są dozwolone. Jeżeli uważasz, że osoba niepełnoletnia przekazała nam dane, skontaktuj się z nami pod adresem contact@dataminder.ai.

18. Profile w mediach społecznościowych

Prowadzimy profile DataMinder w LinkedIn, Facebook i Instagram. Gdy komentujesz, reagujesz lub wysyłasz wiadomość, przetwarzamy dane widoczne w profilu i treść interakcji w celu komunikacji i prowadzenia profilu, na podstawie naszego prawnie uzasadnionego interesu albo – gdy kontakt dotyczy umowy – w celu podjęcia działań na Twoje żądanie lub wykonania umowy.

Operator platformy przetwarza dane na własnych zasadach i może w niektórych przypadkach działać z nami jako współadministrator określonych statystyk lub działań reklamowych. Zapoznaj się również z polityką prywatności właściwej platformy, wskazaną w Załączniku nr 1.

19. Zmiany Polityki

Możemy aktualizować Politykę, gdy zmienia się prawo, usługa, dostawcy, cele przetwarzania lub sposób korzystania z danych. Nowa wersja będzie publikowana z datą obowiązywania. Jeżeli zmiana istotnie wpływa na prawa użytkowników lub sposób przetwarzania, prześlemy dodatkową informację odpowiednią do charakteru zmiany.

20. Dokumenty stanowiące część Polityki

- Załącznik nr 1 – Wykaz narzędzi zewnętrznych;
- Załącznik nr 2 – Cele przetwarzania danych osobowych;
- Załącznik nr 3 – Informacja o wykorzystaniu sztucznej inteligencji;
- Załącznik nr 4 – Polityka cookies.

Załączniki nr 1–4 stanowią integralną część niniejszej Polityki prywatności. W przypadku rozbieżności pierwszeństwo ma postanowienie bardziej szczegółowe dla danego zagadnienia, z uwzględnieniem właściwej umowy i roli DataMinder.

Podstawy prawne i źródła urzędowe

RODO – rozporządzenie (UE) 2016/679: <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pl>

Prawo komunikacji elektronicznej z 12 lipca 2024 r.: <https://eli.gov.pl/eli/DU/2024/1221/ogl/pol>

AI Act – rozporządzenie (UE) 2024/1689: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=pl>

Standardowe klauzule umowne – decyzja wykonawcza Komisji (UE) 2021/914: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=pl

Komisja Europejska – decyzje stwierdzające odpowiedni stopień ochrony i ramy transferowe: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en

Urząd Ochrony Danych Osobowych – informacje o prawach i skargach: <https://uodo.gov.pl/pl/493>

Wykaz narzędzi zewnętrznych Stan na 31 sierpnia 2026 r.

Narzędzie	Dostawca / podmiot umowy	Cel i zakres wykorzystania	Dokumenty dostawcy
Amazon Web Services (AWS)	Amazon Web Services EMEA SARL	Hosting zasadniczej infrastruktury DataMinder w regionie UE (Frankfurt); przechowywanie i przetwarzanie danych kont, projektów, datasetów, plików, wyników i raportów; obsługa kolejek, logów i kopii zapasowych; globalne dostarczanie treści i ochrona ruchu za pomocą usług takich jak CloudFront i WAF.	Polityka prywatności: https://aws.amazon.com/privacy/ AWS DPA i zasady transferów: https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html SCC (warunkowo, gdy dane są transferowane poza EOG do państwa bez decyzji adekwatności): https://aws.amazon.com/service-terms/
Microsoft Foundry / Azure OpenAI	Microsoft Ireland Operations Limited	Obsługa generatywnych funkcji AI, w tym przetwarzanie wiadomości, historii, załączników, opisów i schematów datasetów, statystyk, hipotez, wyników analiz, błędów oraz generowanie interpretacji i raportów.	Informacje prawne Azure: https://azure.microsoft.com/en-us/support/legal/ Microsoft DPA (obejmuje mechanizmy transferowe, w tym SCC): https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA EU Data Boundary i ograniczone transfery operacyjne: https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services
Google Workspace (Gmail, Drive, SMTP)	Google Cloud Poland Sp. z o.o.	Firmowa poczta @dataminder.ai, wysyłanie wiadomości do klientów przez SMTP, komunikacja i przechowywanie korespondencji oraz roboczych materiałów Spółki.	Polityka prywatności: https://policies.google.com/privacy Google Cloud Data Processing Addendum: https://cloud.google.com/terms/data-processing-addendum EU SCC dla Google Workspace: https://cloud.google.com/terms/sccs DPF i pozostałe mechanizmy: https://policies.google.com/privacy/frameworks
Google OAuth	Google Ireland Limited	Opcjonalna rejestracja i logowanie użytkownika za pomocą konta Google.	Polityka prywatności: https://policies.google.com/privacy Google API Services User Data Policy: https://developers.google.com/terms/api-services-user-data-policy DPF i SCC stosowane przez Google: https://policies.google.com/privacy/frameworks
Google Analytics 4 (GA4)	Google Ireland Limited	Analityka korzystania z landing page i aplikacji, w tym ruch, odsłony, interakcje, informacje o urządzeniu oraz identyfikatory online zgodnie z konfiguracją.	Polityka prywatności: https://policies.google.com/privacy Warunki przetwarzania danych Google Analytics: https://support.google.com/analytics/answer/3379636 Warunki transferowe i SCC: https://support.google.com/analytics/answer/9012600 DPF i pozostałe mechanizmy: https://policies.google.com/privacy/frameworks
Stripe	Stripe Technology Europe, Limited	Realizacja jednorazowych płatności i obsługa klienta płatniczego. DataMinder przekazuje adres e-mail oraz imię i nazwisko; użytkownik podaje Stripe dane karty oraz kraj lub region.	Centrum prywatności: https://stripe.com/legal/privacy-center Stripe DPA wraz z Data Transfers Addendum: https://stripe.com/legal/dpa Informacja o DPF i SCC: https://stripe.com/en-be/legal/dpa/faq
Meta Pixel	Meta Platforms Ireland Limited	Pomiar skuteczności kampanii, konwersji i reklam, w zakresie wynikającym z konfiguracji oraz zgody marketingowej użytkownika.	Polityka prywatności: https://www.facebook.com/privacy/policy/ Warunki narzędzi biznesowych Meta Pixel: https://www.facebook.com/legal/terms/businessstools Warunki przetwarzania danych: https://www.facebook.com/legal/terms/dataprocessing EU-US DPF: https://www.facebook.com/privacy/policies/data_privacy_framework/
Sanity CMS / CDN	Sanity.io	Przechowywanie i dostarczanie obrazów artykułów i autorów; przeglądarka odwiedzającego przekazuje do CDN standardowe metadane żądania, w tym adres IP i user-agent.	Polityka prywatności i mechanizmy transferowe (w tym SCC): https://www.sanity.io/legal/privacy Podprocesory: https://www.sanity.io/legal/third-party-sub-processors Warunki: https://www.sanity.io/legal/tos
LinkedIn (profil DataMinder)	LinkedIn Ireland Unlimited Company	Prowadzenie profilu DataMinder oraz obsługa komentarzy i wiadomości kierowanych do profilu.	Polityka prywatności: https://www.linkedin.com/legal/privacy-policy Europejskie informacje o transferach (adekwatność, SCC, DPF): https://www.linkedin.com/legal/privacy/eu Informacja o SCC: https://www.linkedin.com/legal/l/eusccs
Facebook i Instagram (profile DataMinder)	Meta Platforms Ireland Limited	Prowadzenie profili DataMinder oraz obsługa publikacji, komentarzy i wiadomości.	Polityka prywatności: https://www.facebook.com/privacy/policy/ Warunki komercyjne: https://www.facebook.com/legal/commercial_terms EU-US DPF i transfery do Meta Platforms, Inc.: https://www.facebook.com/privacy/policies/data_privacy_framework/
Hotjar	Hotjar Limited	Analiza sposobu korzystania z witryny lub aplikacji, w tym tworzenie map ciepłych oraz analiza kliknięć, przewijania i interakcji, w celu poprawy użyteczności usług DataMinder. Narzędzie jest uruchamiane po uzyskaniu zgody użytkownika na analityczne pliki cookies.	Polityka prywatności i dokumenty prawne: https://www.hotjar.com/legal/ Hotjar DPA (globalny dostęp i SCC dla podprocesorów spoza EOG): https://www.hotjar.com/legal/support/dpa/
Fireflies.ai	Fireflies.ai Corp.	Nagrywanie, transkrypcja, podsumowywanie i sporządzanie notatek ze spotkań po uzyskaniu wymaganej zgody uczestników. Materiały ze spotkań są przechowywane przez DataMinder przez 3 miesiące. W przypadku spotkań obejmujących Dane Powierzone Fireflies.ai działa jako podprocesor.	Polityka prywatności: https://fireflies.ai/privacy-policy DPA i mechanizmy transferowe (deklarowany DPF oraz zapasowe SCC): https://fireflies.ai/data-processing-agreement Podprocesory: https://trust.fireflies.ai/subprocessors Warunki świadczenia usług: https://fireflies.ai/terms-of-service

Cele przetwarzania danych osobowych Stan na 31 sierpnia 2026 r.

Cel przetwarzania	Podstawa prawna przetwarzania	Zakres przetwarzanych danych	Okres przechowywania danych	Źródło pozyskania danych
Założenie i obsługa konta, uwierzytelnianie oraz logowanie przez Google	Art. 6 ust. 1 lit. b RODO – działania na żądanie użytkownika przed zawarciem umowy oraz wykonanie umowy o świadczenie usługi.	Dane identyfikacyjne i kontaktowe, identyfikator konta, adres e-mail, dane uwierzytelniające lub token OAuth, informacje o logowaniu i ustawienia konta.	Przez okres posiadania konta. Po zamknięciu konta dane są usuwane z aktywnych systemów w terminie do 30 dni, z zastrzeżeniem danych wymaganych do rozliczeń, wykonania obowiązków prawnych lub obrony przed roszczeniami. Token Google OAuth jest unieważniany i usuwany z aktywnych systemów po odłączeniu logowania Google albo zamknięciu konta; jego pozostałości w kopiach zapasowych są usuwane w zwykłym cyklu backupów, nie później niż w ciągu 90 dni.	Bezpośrednio od użytkownika; w przypadku Google OAuth – także od Google na podstawie wyboru i autoryzacji użytkownika.
Świadczenie usług! DataMinder: tworzenie projektów, analiza danych oraz generowanie wyników i raportów	Art. 6 ust. 1 lit. b RODO – wykonanie umowy. Jeżeli użytkownik wprowadza dane innych osób, podstawę prawną ustala administrator tych danych.	Dane konta i projektu, pliki i datasety, opisy zmiennych, polecenia, hipotezy, konfiguracje analiz, wyniki, wykresy i raporty; zakres zależy od treści przekazanych przez użytkownika.	W aktywnym koncie bez z góry określonego terminu. Usunięcie projektu lub notebooka powoduje usunięcie jego konfiguracji, wyników i raportów z aktywnych systemów w terminie do 30 dni, lecz nie usuwa datasetu przechowywanego niezależnie w przestrzeni użytkownika. Usunięcie pliku, datasetu albo konta powoduje usunięcie odpowiednich danych z aktywnych systemów w terminie do 30 dni. Dane tymczasowe i cache są usuwane w terminie do 30 dni, automatyczne kopie zapasowe RDS w cyklu nieprzekraczającym 35 dni, a logi i ślady LLM nie później niż w ciągu 90 dni.	Od użytkownika oraz z plików i danych wprowadzonych przez użytkownika.
Realizacja funkcji opartych na sztucznej inteligencji	Art. 6 ust. 1 lit. b RODO – wykonanie umowy. W odniesieniu do danych powierzonych przez klienta – przetwarzanie na jego udokumentowane polecenie zgodnie z art. 28 RODO. Art. 50 AI Act określa obowiązki transparentności, lecz nie stanowi samodzielnej podstawy przetwarzania danych osobowych.	Treść poleceń i rozmów, historia interakcji, załączniki, schematy i statystyki datasetów, hipotezy, wyniki analiz, błędy, interpretacje i raporty; mogą obejmować dane osobowe, jeśli użytkownik je przekaże.	W aktywnym koncie bez z góry określonego terminu, do usunięcia odpowiedniego projektu, notebooka, pliku, datasetu lub konta. Dane są usuwane z aktywnych systemów w terminie do 30 dni od właściwego polecenia usunięcia; logi aplikacyjne i bazodanowe są przechowywane przez 1 miesiąc, a ślady LLM maksymalnie 90 dni. Dane Powierzone nie są wykorzystywane przez DataMinder do trenowania własnych modeli ani własnych badań.	Od użytkownika, z jego projektów i datasetów oraz z wyników działania systemu.
Przetwarzanie datasetów zawierających dane osobowe w imieniu klienta	Art. 28 RODO – DataMinder działa jako podmiot przetwarzający na udokumentowane polecenie klienta; administrator będący klientem odpowiada za podstawę z art. 6 RODO oraz – jeżeli dotyczy – wyjątek z art. 9 ust. 2 RODO.	Dane zawarte w datasetach, plikach i materiałach klienta. Bezpośrednie identyfikatory i niezbędne dane muszą zostać usunięte przed przesłaniem. Dane szczególnych kategorii, dane z art. 10 RODO i dane dzieci są dopuszczalne wyłącznie po minimalizacji i co najmniej pseudonimizacji, bez przekazania DataMinder klucza identyfikacyjnego, jeżeli administrator posiada właściwą podstawę prawną i adekwatne zabezpieczenia. Dane skutecznie zanonimizowane nie podlegają RODO; pseudonimizowane nadal są danymi osobowymi.	W aktywnym koncie zgodnie z poleceniami klienta, bez z góry określonego terminu, do usunięcia właściwego projektu, notebooka, pliku, datasetu lub konta albo zakończenia DPA. Usunięcie projektu nie usuwa datasetu przechowywanego niezależnie w przestrzeni klienta. Po poleceniu usunięcia objęte nim dane są usuwane z aktywnych systemów w terminie do 30 dni. Automatyczne kopie zapasowe RDS są usuwane w cyklu nieprzekraczającym 35 dni, a logi i ślady LLM najpóźniej w ciągu 90 dni, chyba że prawo wymaga dalszego przechowywania.	Od klienta lub osoby działającej w jego imieniu.
Rozliczanie wykorzystania kredytów i funkcji usługi	Art. 6 ust. 1 lit. b RODO – wykonanie umowy.	Identyfikator użytkownika i konta, saldo i historia wykorzystania kredytów, rodzaj i czas operacji oraz powiązane identyfikatory techniczne.	Przez okres posiadania konta. Po zakończeniu umowy – nie dłużej niż do końca roku kalendarzowego, w którym upływa 6 lat od zakończenia umowy lub wymagalności właściwego roszczenia, chyba że właściwy termin przedawnienia jest krótszy albo jego bieg został zawieszony lub przerwany (art. 118–120 Kodeksu cywilnego).	Z systemu DataMinder – na podstawie aktywności użytkownika.
Obsługa płatności, rozliczeń, dokumentów księgowych i obowiązków podatkowych	Art. 6 ust. 1 lit. b RODO – wykonanie umowy; art. 6 ust. 1 lit. c RODO – obowiązki rachunkowe i podatkowe, w szczególności ustawa o rachunkowości i Ordynacja podatkowa.	Dane identyfikacyjne, kontaktowe i rozliczeniowe, informacje o transakcji i płatności, kraj lub region, identyfikatory klienta i płatności Stripe; dane karty są podawane bezpośrednio Stripe.	Dokumentacja księgowa – co do zasady 5 lat, liczonych zgodnie z art. 74 ustawy o rachunkowości; dokumenty podatkowe – do upływu terminu przedawnienia zobowiązania podatkowego, co do zasady 5 lat od końca roku kalendarzowego, w którym upłynął termin płatności (art. 70 § 1 Ordynacji podatkowej). Pozostałe dane płatnicze – nie dłużej niż do końca roku kalendarzowego, w którym upływa 6 lat od transakcji lub zakończenia umowy, jeżeli są niezbędne do obrony przed roszczeniami; stosuje się dłuższy z właściwych terminów ustawowych.	Od użytkownika, z systemu DataMinder oraz od Stripe.
Wysyłanie wiadomości związanych z usługą, kontem i bezpieczeństwem	Art. 6 ust. 1 lit. b RODO – wykonanie umowy; w zakresie ostrzeżeń bezpieczeństwa także art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes polegający na ochronie użytkowników i usługi.	Imię i nazwisko lub nazwa konta, adres e-mail, treść komunikatu, dane o koncie, projekcie, płatności lub zdarzeniu bezpieczeństwa niezbędne do wiadomości.	Przez czas potrzebny do realizacji komunikatu i trwania konta. Jeżeli wiadomość może stanowić dowód wykonania umowy lub zdarzenia bezpieczeństwa – nie dłużej niż do końca roku kalendarzowego, w którym upływa 6 lat od zakończenia umowy lub wysłania wiadomości, chyba że właściwy termin przedawnienia jest krótszy albo jego bieg został zawieszony lub przerwany.	Z konta i aktywności użytkownika oraz z systemów DataMinder.
Obsługa kontaktu, zapytań, wsparcia technicznego i zgłoszeń błędów	Art. 6 ust. 1 lit. b RODO – gdy kontakt dotyczy umowy lub działań przed jej zawarciem; art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes polegający na obsłudze korespondencji, wsparciu i doskonaleniu usługi.	Dane kontaktowe, treść korespondencji i załączników, informacje o koncie, projekcie, urządzeniu, przeglądanie, błędzie i czynnościach użytkownika – w zakresie potrzebnym do sprawy.	Do zakończenia sprawy. Następnie dokumentacja sprawy – nie dłużej niż do końca roku kalendarzowego, w którym upływa 6 lat od zamknięcia zgłoszenia lub wymagalności właściwego roszczenia, chyba że właściwy termin jest krótszy albo jego bieg został zawieszony lub przerwany.	Bezpośrednio od osoby kontaktującej się oraz z systemów DataMinder w związku ze zgłoszeniem.
Obsługa reklamacji, odstąpienia od	Art. 6 ust. 1 lit. b i c RODO – wykonanie umowy i obowiązki	Dane identyfikacyjne, kontaktowe, konta, zamówienia i	Przez czas obsługi sprawy, a następnie do upływu właściwego terminu	Od użytkownika, z systemów DataMinder i

Cel przetwarzania	Podstawa prawna przetwarzania	Zakres przetwarzanych danych	Okres przechowywania danych	Źródło pozyskania danych
umowy, zwrotów i sporów płatniczych	wynikające min. z ustawy o prawach konsumenta; art. 6 ust. 1 lit. f RODO – ustalenie, dochodzenie lub obrona roszczeń.	płatności, treść ządania, korespondencja, dowody wykonania usługi oraz dane niezbędne do rozstrzygnięcia sprawy.	przedawnienia roszczeń oraz wymaganej retencji księgowej lub podatkowej.	od Stripe; ewentualnie od banku lub operatora płatności w związku ze sporem.
Zapewnienie bezpieczeństwa, diagnostyka, zapobieganie nadużyciom i wykazanie zgodności	Art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes polegający na ochronie usługi, użytkowników i danych oraz dochodzeniu roszczeń; w zakresie wykonania obowiązków bezpieczeństwa – art. 6 ust. 1 lit. c w zw. z art. 5 ust. 2 i art. 32 RODO.	Adres IP, znaczniki czasu, identyfikatory konta, sesji, urządzenia i ządania, logi aplikacyjne i bezpieczeństwa, informacje o błędach i nietypowej aktywności.	Logi aplikacyjne, uwierzytelniania, błędów, dostępu i bezpieczeństwa, w tym logi Lambda i bazy danych, są przechowywane przez 1 miesiąc. Ślady LLM w self-hosted Langfuse są przechowywane maksymalnie 90 dni. Informacje wyodrębnione z logów jako dokumentacja konkretnego incydentu, nadużycia lub postępowania mogą być przechowywane do zakończenia sprawy, a następnie do upływu właściwego terminu przedawnienia roszczeń lub zakończenia postępowania.	Automatycznie z urządzenia, przeglądarki, aplikacji i infrastruktury DataMinder.
Prowadzenie listy oczekujących oraz informowanie o dostępności usługi	Art. 6 ust. 1 lit. a RODO – zgoda. Jeżeli wiadomość ma charakter informacji handlowej lub marketingu bezpośredniego, dodatkowo wymagana jest uprzednia zgoda zgodnie z art. 398 Prawa komunikacji elektronicznej.	Adres e-mail, data i treść zgody, ewentualnie imię oraz informacje o zainteresowaniu usługą.	Do wycofania zgody, rezygnacji z listy albo zakończenia celu listy oczekujących. Dowód udzielenia i wycofania zgody – nie dłużej niż do końca roku kalendarzowego, w którym upływa 6 lat od wycofania zgody lub zakończenia celu, o ile jest potrzebny do wykazania zgodności lub obrony przed roszczeniami.	Bezpośrednio od osoby zapisującej się na listę.
Wysyłka newslettera i komunikacji marketingowej e-mail	Art. 6 ust. 1 lit. a RODO – zgoda; art. 398 Prawa komunikacji elektronicznej – uprzednia zgoda na przysyłanie informacji handlowej, w tym marketingu bezpośredniego.	Adres e-mail, imię – jeżeli podane, data i treść zgody, historia wysyłek, otwarć i kliknięć – jeżeli pomiar jest aktywny.	Do wycofania zgody lub rezygnacji. Następnie minimalne dane na liście blokującej przez czas niezbędny do respektowania sprzeciwu, a dowód udzielenia i wycofania zgody – nie dłużej niż do końca roku kalendarzowego, w którym upływa 6 lat od wycofania zgody lub ostatniej wysyłki, o ile jest potrzebny do wykazania zgodności lub obrony przed roszczeniami.	Bezpośrednio od subskrybenta; dane o interakcjach – z systemu wysyłkowego.
Rekrutacja i obsługa udziału testerów w testach DataMinder	Art. 6 ust. 1 lit. a RODO – zgoda, a gdy udział odbywa się na podstawie uzgodnienia lub umowy – art. 6 ust. 1 lit. b RODO.	Dane identyfikacyjne i kontaktowe, informacje o profilu testera, dostępności i przebiegu testów, opinie, zgłoszenia, odpowiedzi i materiały przekazane podczas testów.	Do zakończenia testów i rozliczenia udziału. Następnie – nie dłużej niż do końca roku kalendarzowego, w którym upływa 6 lat od zakończenia testów, rozliczenia albo wycofania zgody, chyba że właściwy termin przedawnienia jest krótszy. Materiały niewymagane do rozliczeń lub obrony przed roszczeniami usuwa się wcześniej.	Bezpośrednio od testera oraz z jego aktywności w DataMinder.
Nagrywanie, transkrypcja i sporządzanie notatek ze spotkań	Art. 6 ust. 1 lit. a RODO – zgoda uczestnika. Jeżeli treść ujawnia szczególne kategorie danych, konieczne jest również spełnienie odpowiedniej przesłanki z art. 9 ust. 2 RODO, co wymaga odrębnej oceny.	Głos, wizerunek – jeśli rejestrowany, dane identyfikacyjne i kontaktowe, treść wypowiedzi, transkrypcja, notatki, podsumowania i metadane spotkania.	Nagrania, transkrypcje, podsumowania i notatki ze spotkań są przechowywane przez 3 miesiące od dnia spotkania. Po tym okresie są usuwane, chyba że uczestnik wcześniej wycofa zgodę i nie istnieje inna podstawa dalszego przechowywania albo zachowanie konkretnego materiału jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń. Po zleceniu usunięcia w Fireflies trwałe usunięcie danych jest realizowane zgodnie z procedurą dostawcy, nie później niż w ciągu 30 dni.	Od uczestników spotkania oraz automatycznie z narzędzia rejestrującego spotkanie.
Analityka korzystania z serwisu i badanie użyteczności (Google Analytics 4 i Hotjar)	Art. 6 ust. 1 lit. a RODO – zgoda; art. 399 Prawa komunikacji elektronicznej – uprzednia zgoda na przechowywanie informacji lub uzyskanie dostępu do informacji w urządzeniu końcowym, jeżeli technologia nie jest ściśle niezbędna.	Identyfikatory internetowe i urządzenia, adres IP w zakresie wynikającym z konfiguracji, przybliżona lokalizacja, dane o przeglądaniu i urządzeniu, odsłony, kliknięcia, przewijanie, nawigacja i inne zdarzenia; w Hotjar także nagrania sesji lub mapy cieplne zgodnie z konfiguracją i maskowaniem.	Do wycofania zgody w zakresie dalszego zbierania. Dane użytkowników i zdarzeń w Google Analytics 4 są przechowywane maksymalnie przez 14 miesięcy. Nagrania sesji i dane map cieplnych Hotjar są przechowywane maksymalnie przez 365 dni od ich zarejestrowania, po czym dostawca rozpoczyna ich automatyczne usuwanie, także z kopii zapasowych. Dane wpisywane w formularzach są maskowane. Wycofanie zgody powoduje zaprzestanie dalszego zbierania danych.	Automatycznie z urządzenia i aktywności użytkownika – dopiero po uzyskaniu wymaganej zgody.
Pomiar skuteczności kampanii i reklam (Meta Pixel)	Art. 6 ust. 1 lit. a RODO – zgoda; art. 399 Prawa komunikacji elektronicznej – zgoda na dostęp lub zapis informacji w urządzeniu. W przypadku bezpośredniej komunikacji marketingowej stosuje się również art. 398 tej ustawy.	Identyfikatory online i reklamowe, adres IP, dane o przeglądaniu i urządzeniu, odwiedzone strony, zdarzenia konwersji i interakcje z reklamą; dodatkowe dane tylko w zakresie wynikającym z aktywnej konfiguracji.	Do wycofania zgody w zakresie dalszego zbierania danych. Po odmowie lub wycofaniu zgody Meta Pixel nie przekazuje nowych zdarzeń. Dane przekazane wcześniej są przechowywane przez Meta przez okres zależny od rodzaju wykorzystywanej funkcji reklamowej, potrzeb pomiaru i bezpieczeństwa oraz obowiązków prawnych dostawcy. DataMinder przechowuje dostępne raporty kampanii przez okres prowadzenia i rozliczenia kampanii, a następnie tylko tak długo, jak są potrzebne do analizy skuteczności marketingu lub obrony przed roszczeniami.	Automatycznie z urządzenia i aktywności użytkownika – dopiero po uzyskaniu wymaganej zgody; także od Meta w zakresie raportów kampanii.
Prowadzenie profili DataMinder i obsługa kontaktu w LinkedIn, Facebook i Instagram	Art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes polegający na komunikacji, prowadzeniu profili i budowaniu relacji; art. 6 ust. 1 lit. b RODO – gdy kontakt dotyczy umowy lub działań przed jej zawarciem.	Nazwa profilu, imię i nazwisko, publiczne informacje profilu, komentarze, reakcje, wiadomości i inne dane przekazane w serwisie społecznościowym.	Przez czas obsługi kontaktu i prowadzenia profilu. Wewnętrzne kopie wiadomości lub eksporty wykorzystywane jako dowód – nie dłużej niż do końca roku kalendarzowego, w którym upływa 6 lat od zakończenia kontaktu, chyba że właściwy termin przedawnienia jest krótszy; dane pozostające na platformie podlegają również zasadom jej operatora.	Od osoby korzystającej z platformy oraz od operatora właściwego serwisu społecznościowego.
Obsługa żądań wynikających z praw os. ob., których dane dotyczą	Art. 6 ust. 1 lit. c RODO – wykonanie obowiązków z art. 12–22 RODO; w zakresie dokumentowania obsługi i obrony przed roszczeniami także art. 6 ust. 1 lit. f RODO.	Dane identyfikacyjne i kontaktowe, dane służące weryfikacji tożsamości, treść ządania, korespondencja, informacje o podjętych działaniach i objętych nimi danych.	Przez czas obsługi ządania. Dokumentacja sposobu jego rozpatrzenia – nie dłużej niż do końca roku kalendarzowego, w którym upływa 6 lat od udzielenia ostatecznej odpowiedzi, o ile jest potrzebna do wykazania zgodności lub obrony przed roszczeniami; dłużej wyłącznie w razie trwającego postępowania.	Od osoby składającej żądanie, jej pełnomocnika oraz z systemów DataMinder.
Ustalenie, dochodzenie i obrona roszczeń	Art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes polegający na ochronie praw DataMinder i obronie przed roszczeniami.	Dane dotyczące konta, umowy, płatności, korzystania z usługi, komunikacji, zgłoszeń, logów i zdarzeń – w zakresie niezbędnym dla danego roszczenia.	Do upływu właściwego terminu przedawnienia roszczenia, a w razie sporu – do prawomocnego zakończenia postępowania i wykonania rozstrzygnięcia.	Od osoby, której sprawa dotyczy, z systemów DataMinder, od dostawców płatności lub usług oraz – jeżeli dotyczy –

Cel przetwarzania	Podstawa prawna przetwarzania	Zakres przetwarzanych danych	Okres przechowywania danych	Źródło pozyskania danych
Rejestrowanie i wykazywanie zgód oraz preferencji prywatności	Art. 6 ust. 1 lit. c RODO w zw. z art. 5 ust. 2 i art. 7 ust. 1 RODO – obowiązek wykazania zgodności; w zakresie zgód na technologie i komunikację także art. 398–399 Prawa komunikacji elektronicznej.	Identyfikator użytkownika lub urządzenia, rodzaj i treść zgody, data i czas wyboru, wersja komunikatu, preferencje, informacja o wycofaniu lub zmianie zgody.	Przez okres obowiązywania preferencji. Dowód udzielenia, odmowy, zmiany lub wycofania zgody – nie dłużej niż do końca roku kalendarzowego, w którym upływa 6 lat od ostatniej zmiany lub wycofania zgody, o ile jest potrzebny do wykazania zgodności lub obrony przed roszczeniami. Minimalny wpis na liście blokującej może być utrzymywany tak długo, jak jest to konieczne do respektowania sprzeciwu.	od organów, sądów i pełnomocników. Bezpośrednio z wyboru użytkownika i automatycznie z mechanizmu zarządzania zgodami.

ZAŁĄCZNIK NR 3

Informacja o wykorzystaniu sztucznej inteligencji

Stan na 31 sierpnia 2026 r.

1. Czym są funkcje AI w DataMinder

DataMinder wykorzystuje systemy sztucznej inteligencji jako warstwę wspierającą korzystanie z usługi analizy danych. Użytkownik jest informowany, że korzysta z funkcji AI, w interfejsie właściwej funkcji. Rozwiązania AI wspierają w szczególności:

- prowadzenie czatu i doprecyzowanie problemu badawczego;
- formułowanie i doprecyzowanie hipotez;
- tworzenie tekstowych wyjaśnień, interpretacji i raportów na podstawie wyników obliczeń;
- generowanie tytułów, opisów, treści pomocniczych i elementów projektu;
- objaśnianie błędów oraz prezentację wyników analiz.

Obliczenia statystyczne są wykonywane przez odrębny, deterministyczny komponent. Model językowy nie jest źródłem wartości statystyk ani wyników testów statystycznych; otrzymuje wyniki obliczeń, aby przedstawić je i objaśnić w formie tekstowej.

2. Dostawca i wykorzystywany komponent

Do obsługi generatywnych funkcji AI DataMinder wykorzystuje Microsoft Foundry / Azure OpenAI. Podmiotem umownym wskazanym w dokumentacji DataMinder jest Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irlandia. Wykorzystywany jest model z rodziny GPT.

Dane są przekazywane do dostawcy wyłącznie w zakresie niezbędnym do wykonania funkcji uruchomionej przez użytkownika. Aktualne informacje o dostawcy i jego dokumentach znajdują się w Załączniku nr 1 do Polityki prywatności – Wykaz narzędzi zewnętrznych.

Wdrożenie Azure OpenAI przypisane do DataMinder działa w EU Data Zone Standard. Dane wejściowe i wyjściowe modelu są przetwarzane w granicach tej strefy danych zgodnie z konfiguracją usługi. Microsoft przewiduje ograniczone przypadki globalnego dostępu lub transferu związane m.in. z bezpieczeństwem, wsparciem i utrzymaniem usług; zastosowanie mają wówczas mechanizmy i zabezpieczenia przewidziane w Microsoft DPA oraz rozdziale V RODO.

3. Jakie informacje mogą być przetwarzane przez funkcje AI

- wiadomości, pytania i polecenia użytkownika oraz historia rozmowy;
- załączniki oraz informacje wydobyte z przesłanych plików;
- opisy datasetów, nazwy i typy pól, schematy, statystyki i próbki wartości;
- hipotezy, kontekst projektu, wyniki analiz i informacje o błędach;
- wygenerowane odpowiedzi, raporty, tekst, kod oraz metadane techniczne wykonania.

Zakres zależy od treści przekazanych przez użytkownika. Materiały mogą zawierać dane osobowe, informacje poufne lub dane pochodzące z datasetu klienta. Użytkownik powinien przekazywać wyłącznie informacje niezbędne do danego celu i – jeżeli działa jako administrator danych – posiadać odpowiednią podstawę ich przetwarzania.

Przed przekazaniem danych użytkownik usuwa bezpośrednio identyfikatory oraz dane zbędne dla analizy. Dane szczególnych kategorii, dane dotyczące wyroków skazujących i naruszeń prawa oraz dane dzieci mogą być przetwarzane wyłącznie po minimalizacji i co najmniej pseudonimizacji, bez przekazania DataMinder klucza identyfikacyjnego, jeżeli użytkownik posiada właściwą podstawę prawną i zastosował zabezpieczenia adekwatne do ryzyka. Dane prawidłowo zanonimizowane nie są danymi osobowymi; pseudonimizowane nadal podlegają RODO.

4. Role i odpowiedzialność za dane

W odniesieniu do danych konta, rozliczeń, bezpieczeństwa i własnych celów operacyjnych DataMinder działa jako administrator danych. W odniesieniu do danych osobowych zawartych w datasecie klienta DataMinder co do zasady działa jako podmiot przetwarzający na udokumentowane polecenie klienta, zgodnie z art. 28 RODO i właściwą umową powierzenia.

Klient jako administrator odpowiada w szczególności za legalność pozyskania danych, podstawę prawną, spełnienie obowiązków informacyjnych wobec osób, ustalenie właściwego okresu przechowywania oraz zgodność zamierzonego zastosowania wyników.

DataMinder odpowiada za obowiązki dotyczące wdrożenia i stosowania funkcji AI w zakresie wynikającym z roli przypisanej mu przez AI Act. Ocena roli zależy od konkretnej funkcji, sposobu integracji, przeznaczenia i zmian wprowadzanych w systemie i jest aktualizowana wraz ze zmianą tych elementów.

5. Przezystość i oznaczenie działania AI

Funkcje przeznaczone do bezpośredniej interakcji z użytkownikiem powinny jasno wskazywać, że odpowiedź lub treść jest generowana przez AI, chyba że jest to oczywiste dla rozsądnie poinformowanej, uważnej i ostrożnej osoby w danych okolicznościach. Informacja powinna zostać przekazana najpóźniej przy rozpoczęciu interakcji.

Obowiązek ten wynika z art. 50 ust. 1 AI Act, mającego zastosowanie od 2 sierpnia 2026 r. Zakres obowiązków dotyczących technicznego oznaczania treści generowanych lub modyfikowanych przez AI wymaga odrębnej oceny na podstawie art. 50 ust. 2 AI Act oraz aktualnych wytycznych Komisji Europejskiej.

Interfejs funkcji przeznaczonych do bezpośredniej interakcji wskazuje użytkownikowi, że korzysta on z AI. Treści generowane lub modyfikowane przez AI są oznaczane w zakresie wymaganym przez art. 50 AI Act, z uwzględnieniem rodzaju treści i sposobu jej udostępnienia.

6. Nadzór człowieka i sposób korzystania z wyników

- wyniki AI mają charakter pomocniczy i mogą wymagać weryfikacji przez użytkownika;
- użytkownik powinien sprawdzić poprawność danych wejściowych, założeń, interpretacji i wygenerowanego raportu;
- wyniku AI nie należy traktować jako profesjonalnej porady prawnej, medycznej, finansowej ani innej porady specjalistycznej;
- w razie rozbieżności pierwszeństwo mają wyniki deterministycznych obliczeń statystycznych, a nie tekstowe objaśnienie modelu językowego.

Zgodnie z obecnym opisem funkcji DataMinder nie wykorzystuje AI do podejmowania wobec użytkownika decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, które wywołują skutki prawne lub w podobny sposób istotnie na niego wpływają. Jeżeli sposób użycia produktu ulegnie zmianie, konieczna będzie ponowna ocena art. 22 RODO oraz klasyfikacji AI Act.

7. Ograniczenia i niedozwolone zastosowania

Treści generowane przez AI mogą być niepełne, niedokładne, nieaktualne albo nieadekwatne do kontekstu. Samo występowanie nadzoru człowieka nie usuwa ryzyka błędu ani nie przesądza o zgodności konkretnego zastosowania z prawem.

Bez uprzedniej, udokumentowanej oceny prawnej, ryzyka i zabezpieczeń DataMinder nie powinien być używany do podejmowania lub wspierania decyzji dotyczących konkretnych osób w obszarach takich jak:

- rekrutacja, zatrudnienie, ocena pracowników lub zakończenie współpracy;
- przyjęcie do edukacji, ocenianie uczniów lub studentów;
- dostęp do kredytu, ubezpieczenia, świadczeń publicznych lub podstawowych usług;
- diagnostyka, leczenie lub inne decyzje medyczne;
- profilowanie ryzyka, scoring osób, egzekwowanie prawa albo wymiar sprawiedliwości;

- rozpoznawanie emocji, kategoryzacja biometryczna lub inne zastosowania mogące podlegać zakazom albo reżimowi wysokiego ryzyka AI Act.

8. Trenowanie, ulepszanie produktu i retencja

Zgodnie z publicznymi informacjami Microsoft dane klientów Azure OpenAI nie są wykorzystywane do trenowania bazowych modeli dostawcy bez zgody klienta. Publiczna deklaracja dostawcy nie zastępuje weryfikacji warunków i ustawień obowiązujących dla konkretnego konta DataMinder.

DataMinder przetwarza prompty, odpowiedzi i metadane w zakresie potrzebnym do świadczenia funkcji AI, rozliczania wykorzystania, diagnostyki, bezpieczeństwa i generowania raportów. Dane Powierzone przez klienta nie są wykorzystywane przez DataMinder do trenowania własnych modeli, benchmarków, badań, marketingu ani ulepszania produktu bez odrębnego zgodnego z prawem uzgodnienia. Podstawy prawne, cele i okresy przechowywania opisuje Polityka prywatności oraz Załącznik nr 2 – Cele przetwarzania danych osobowych.

Prompty, odpowiedzi i dane projektu pozostają w aktywnym koncie do ich usunięcia zgodnie z poleceniem użytkownika. Logi aplikacyjne i bazodanowe są przechowywane przez 1 miesiąc, ślady LLM maksymalnie 90 dni, a automatyczne kopie zapasowe RDS w cyklu nieprzekraczającym 35 dni. Szczegółowe kryteria retencji zawiera Załącznik nr 2.

9. Bezpieczeństwo i minimalizacja danych

Użytkownik powinien przed przestaniem danych ograniczyć ich zakres do minimum potrzebnego do analizy, a jeżeli jest to możliwe – usunąć bezpośrednio identyfikatory, zastosować pseudonimizację i nie umieszczać danych osobowych w nazwach projektów, pól ani poleceniach. Pseudonimizacja nie oznacza anonimizacji i nie wyłącza stosowania RODO.

DataMinder stosuje środki techniczne i organizacyjne opisane w dokumentacji usługi. Szczegółowych parametrów bezpieczeństwa nie należy wywodzić z niniejszej informacji; obowiązujące zobowiązania wynikają z właściwej umowy i dokumentacji bezpieczeństwa.

10. Prawa osób i kontakt

Informacje o administratorze, podstawach prawnych, odbiorcach, transferach, retencji oraz prawach osób znajdują się w Polityce prywatności i jej pozostałych załącznikach. Jeżeli DataMinder przetwarza dane na zlecenie klienta, żądania osób dotyczące datasetu klienta są obsługiwane zgodnie z rolami określonymi w umowie powierzenia.

Pytania dotyczące wykorzystania AI lub danych osobowych można kierować na adres: contact@dataminder.ai.

Podstawy regulacyjne i materiały urzędowe

AI Act – rozporządzenie (UE) 2024/1689, w szczególności art. 4, art. 5, art. 50 i art. 113: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=pl>

Komisja Europejska – Wytyczne w sprawie obowiązków przejrzystości z art. 50 AI Act, 20 lipca 2026 r.: <https://digital-strategy.ec.europa.eu/pl/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems>

Microsoft EU Data Boundary – ograniczone transfery dla wszystkich usług: <https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services>

Microsoft Products and Services Data Protection Addendum: <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>

RODO – rozporządzenie (UE) 2016/679, w szczególności art. 5, 6, 9, 13–14, 22, 25, 28 i 32: <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pl>

ZAŁĄCZNIK NR 4

Polityka cookies Wersja DM-COOKIE-310826-PL | stan na 31 sierpnia 2026 r.

1. Zakres dokumentu

Niniejsza Polityka wyjaśnia, w jaki sposób DataMinder sp. z o.o. wykorzystuje pliki cookies, pamięć lokalną, pamięć sesyjną i podobne technologie w serwisach oraz aplikacji DataMinder. Stanowi uzupełnienie Polityki prywatności i wykazu narzędzi zewnętrznych.

Administratorem danych osobowych związanych z wykorzystaniem tych technologii dla własnych celów jest DataMinder sp. z o.o. z siedzibą przy ul. Lipnowskiej 207, 09-400 Maszewo Duże. Kontakt: contact@dataminder.ai.

2. Czym są cookies i podobne technologie

Cookies są niewielkimi informacjami zapisywanymi w przeglądarce. W podobny sposób działa pamięć lokalna i pamięć sesyjna przeglądarki. Technologie te mogą służyć do utrzymania logowania, zapamiętania ustawień, zabezpieczenia płatności, pomiaru korzystania z serwisu oraz oceny skuteczności kampanii.

Okres wskazany poniżej oznacza maksymalny czas pozostawiania informacji w urządzeniu. Użytkownik może usunąć ją wcześniej. Czas przechowywania danych po stronie dostawcy może być inny i jest opisany w dokumentacji dostawcy oraz - w zakresie danych osobowych - w Polityce prywatności.

3. Zasady udzielania i wycofywania zgody

Technologie niezbędne są wykorzystywane bez odrębnej zgody wyłącznie w zakresie koniecznym do transmisji, świadczenia funkcji wyraźnie żądanej przez użytkownika, uwierzytelniania, bezpieczeństwa albo zapamiętania wyboru dotyczącego prywatności.

Google Analytics 4, Hotjar i Meta Pixel pozostają wyłączane do czasu udzielenia odpowiedniej zgody. Nie wysyłają danych przed zgodą, po odmowie ani po jej wycofaniu. Zgody analityczne i marketingowe są od siebie oddzielone.

Zgodę można w każdej chwili zmienić lub wycofać, ponownie otwierając panel ustawień cookies dostępny w serwisie. Wycofanie zgody nie wpływa na zgodność z prawem wcześniejszego przetwarzania. Odmowa nie ogranicza dostępu do podstawowych funkcji DataMinder.

Dla technologii opcjonalnych podstawą prawną jest zgoda wymagana przez art. 399 Prawa komunikacji elektronicznej oraz - gdy dochodzi do przetwarzania danych osobowych - art. 6 ust. 1 lit. a RODO. Dla technologii niezbędnych zastosowanie ma wyjątek przewidziany w art. 399 ust. 3 Prawa komunikacji elektronicznej, a podstawą przetwarzania danych osobowych jest odpowiednio wykonanie umowy lub prawnie uzasadniony interes polegający na zapewnieniu bezpieczeństwa i prawidłowego działania usługi.

4. Technologie wykorzystywane przez DataMinder

4.1. Technologie niezbędne i ustawienia wybrane przez użytkownika

Technologia	Cel i zakres	Okres działania
Cookie uwierzytelniające DataMinder	Utrzymanie zalogowanej sesji, uwierzytelnianie i ochrona konta.	do 30 dni
Ustawienia interfejsu	Zapamiętanie ustawienia interfejsu wybranego przez użytkownika.	do 7 dni

Technologia	Cel i zakres	Okres działania
Preferencja języka	Zapamiętanie wybranego języka serwisu.	do 1 roku
Wybór dotyczący cookies - pamięć lokalna	Zapisanie udzielonej, odmówionej lub wycofanej zgody, aby respektować wybór użytkownika.	do zmiany wyboru lub wyczyszczenia pamięci przeglądarki
Stan zakładek - pamięć lokalna	Zachowanie stanu elementów interfejsu wybranego przez użytkownika.	do zmiany ustawienia lub wyczyszczenia pamięci przeglądarki
Stripe: __stripe_mid	Zapobieganie oszustwom i ocena ryzyka podczas płatności realizowanej na żądanie użytkownika.	do 1 roku
Stripe: __stripe_sid	Zapobieganie oszustwom i ochrona bieżącej sesji płatniczej.	do 30 minut
Stripe: _ab, _mf - pamięć sesyjna	Ochrona płatności i wykrywanie nadużyć na stronie Stripe.	do końca sesji

Cookies Stripe są uruchamiane w związku z rozpoczęciem płatności. Stripe może stosować również inne niezbędne zabezpieczenia zależnie od metody płatności, urządzenia i mechanizmów przeciwdziałania oszustwom.

4.2. Analityka i badanie użyteczności

Poniższe technologie są uruchamiane wyłącznie po udzieleniu zgody analitycznej.

Technologia	Cel i zakres	Okres działania
GA4: _ga	Rozróżnianie użytkowników oraz pomiar korzystania z serwisu.	domyślnie do 2 lat; przeglądarka może skrócić ten okres
GA4: _ga_<identyfikator>	Utrzymanie informacji o sesji i przypisanie zdarzeń do właściwej sesji.	domyślnie do 2 lat; przeglądarka może skrócić ten okres
Hotjar: _hjSessionUser_<site_id>	Przypisanie kolejnych wizyt w DataMinder do pseudonimowego identyfikatora właściwego tylko dla serwisu DataMinder.	do 365 dni
Hotjar: _hjSession_<site_id>	Utrzymanie danych bieżącej sesji potrzebnych do tworzenia map cieplnych i analizy interakcji.	30 minut, przedłużane przy aktywności
Hotjar: cookies i pamięć testowa	Sprawdzenie obsługi cookies oraz pamięci lokalnej i sesyjnej, a także parametrów widoku. Obejmuje m.in. _hjCookieTest, _hjLocalStorageTest, _hjSessionStorageTest i _hjTLDTTest.	sesja albo usunięcie niemal natychmiast po teście

4.3. Pomiar kampanii i marketing

Poniższe technologie są uruchamiane wyłącznie po udzieleniu zgody marketingowej.

Technologia	Cel i zakres	Okres działania
Meta Pixel: _fbp	Rozpoznanie przeglądarki na potrzeby pomiaru reklam, konwersji, analityki marketingowej i - zgodnie z konfiguracją - remarketingu.	do 90 dni
Meta Pixel: _fbclid	Zapamiętanie identyfikatora kliknięcia reklamy Meta, jeżeli użytkownik przeszedł do DataMinder z reklamy zawierającej taki identyfikator.	do 90 dni

5. Jakie dane mogą być przetwarzane

W zależności od technologii mogą być przetwarzane: identyfikator cookie lub urządzenia, adres IP, data i godzina wizyty, odwiedzone podstrony, kliknięcia, przewijanie, parametry sesji, informacje o przeglądarce, systemie operacyjnym i urządzeniu, przybliżona lokalizacja, źródło wejścia oraz informacje o skuteczności kampanii. DataMinder nie przesyła do narzędzi analitycznych i marketingowych treści datasetów ani bezpośrednich identyfikatorów użytkownika.

6. Dostawcy i transfery

Dostawcami technologii opisanych w niniejszej Polityce są w szczególności Google Ireland Limited, Hotjar Limited, Meta Platforms Ireland Limited oraz Stripe Technology Europe, Limited. Szczegółowe informacje o podmiotach, celach, dokumentach dostawców i możliwych transferach poza EOG znajdują się w Załączniku nr 1 do Polityki prywatności.

7. Zarządzanie technologiami w przeglądarce

Oprócz panelu ustawień cookies użytkownik może usunąć lub zablokować cookies w ustawieniach przeglądarki. Zablokowanie technologii niezbędnych może spowodować, że logowanie, ustawienia, płatności albo inne funkcje nie będą działały prawidłowo. Usunięcie cookies z poziomu przeglądarki nie zawsze usuwa dane wcześniej przesłane dostawcy.

8. Zmiany Polityki i kontakt

Polityka może być aktualizowana, gdy zmieni się prawo, konfiguracja serwisu, wykorzystywane technologie albo dostawcy. Aktualna wersja jest publikowana w serwisie DataMinder. Pytania dotyczące cookies i ochrony danych można kierować na contact@dataminder.ai.

9. Dokumentacja dostawców

- Google Analytics - cookies GA4: <https://support.google.com/analytics/answer/11397207>
- Hotjar - cookies kodu śledzącego: <https://help.hotjar.com/hc/en-us/articles/36819973371409-Cookies-Set-by-the-Hotjar-Tracking-Code>
- Meta - polityka cookies: <https://www.facebook.com/privacy/policies/cookies/>
- Stripe - ustawienia i wykaz cookies: <https://stripe.com/cookie-settings>