Jak zadbać o swoją prywatność, używając Androida

Jak bardzo trzeba się postarać, by ograniczyć ilość danych zbieranych przez producentów urządzeń z Androidem i firmę Google, która regularnie wydaje nowe wersje systemu? Pokazujemy krok po kroku, co trzeba zrobić, by zapewnić sobie więcej prywatności.

Twórcy Androida umieścili „Menedżera uprawnień” wśród ustawień mających wpływ na prywatność i rzeczywiście, szafując uprawnieniami na prawo i lewo, możemy nieopatrznie dać aplikacjom zbyt szeroki dostęp do naszych danych, tracąc tym samym część prywatności. Jak temu zaradzić, opisywaliśmy w jednym z wcześniejszych artykułów, w tym skupimy się więc na innych opcjach, które warto wziąć pod uwagę. Jak je skonfigurować, omówimy na przykładzie Galaxy M21 od Samsunga, działającego pod kontrolą Androida 11 z interfejsem One UI 3.1. Sprawdzimy też, co dodano w Androidzie 12 z One UI 4.1. Układ ustawień w telefonach z inną wersją systemu bądź nakładką innego producenta może odbiegać od tego, który pokazujemy, wiele opcji będzie jednak podobnych.

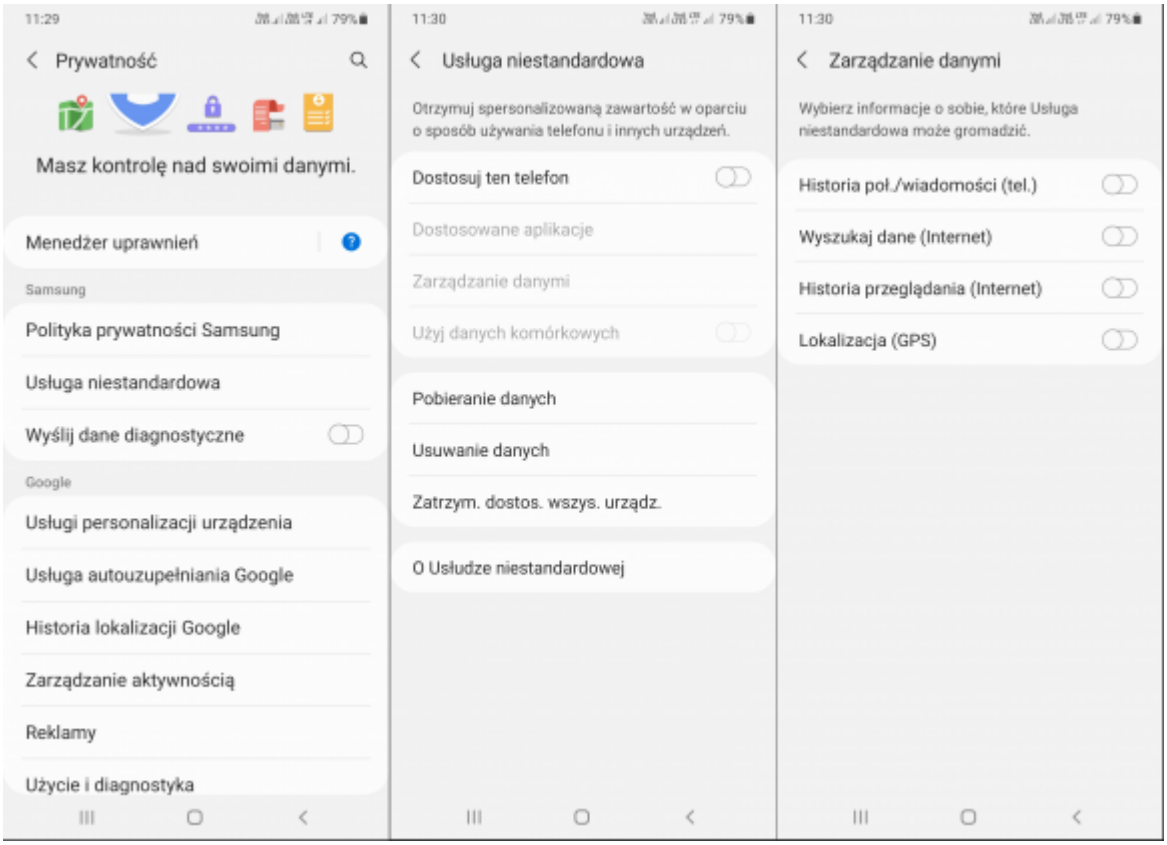
Jakie dane zbiera Samsung i co z tym zrobić

W polityce prywatności Samsung przyznaje, że „gromadzi informacje osobiste Użytkownika różnymi sposobami”. Interesują go zarówno dane przekazywane bezpośrednio, np. podczas

zakładania konta, zakupu którejś z płatnych usług czy kontaktu z obsługą klienta, jak i zbierane przez firmowe aplikacje, gdy korzystamy z naszego telefonu. W tym drugim przypadku chodzi nie tylko o podstawowe informacje o urządzeniu (jak model, IMEI, MAC, wersja systemu operacyjnego, numer telefonu czy adres IP), ale też o pliki cookie, dane pochodzące z logów, historię obejrzanych treści, nagrania naszego głosu (jeśli stosujemy polecenia głosowe), słowa wpisywane za pomocą klawiatury (gdy włączymy funkcję podpowiadania tekstu), informacje o lokalizacji itp. Jakby tego było mało, Samsung zbiera dane „dostępne publicznie lub za opłatą", np. pochodzące z mediów społecznościowych – są one następnie łączone z innymi informacjami o użytkowniku danego smartfona. Firma nie stroni też od usług analitycznych zewnętrznych dostawców, jak Google Analytics.

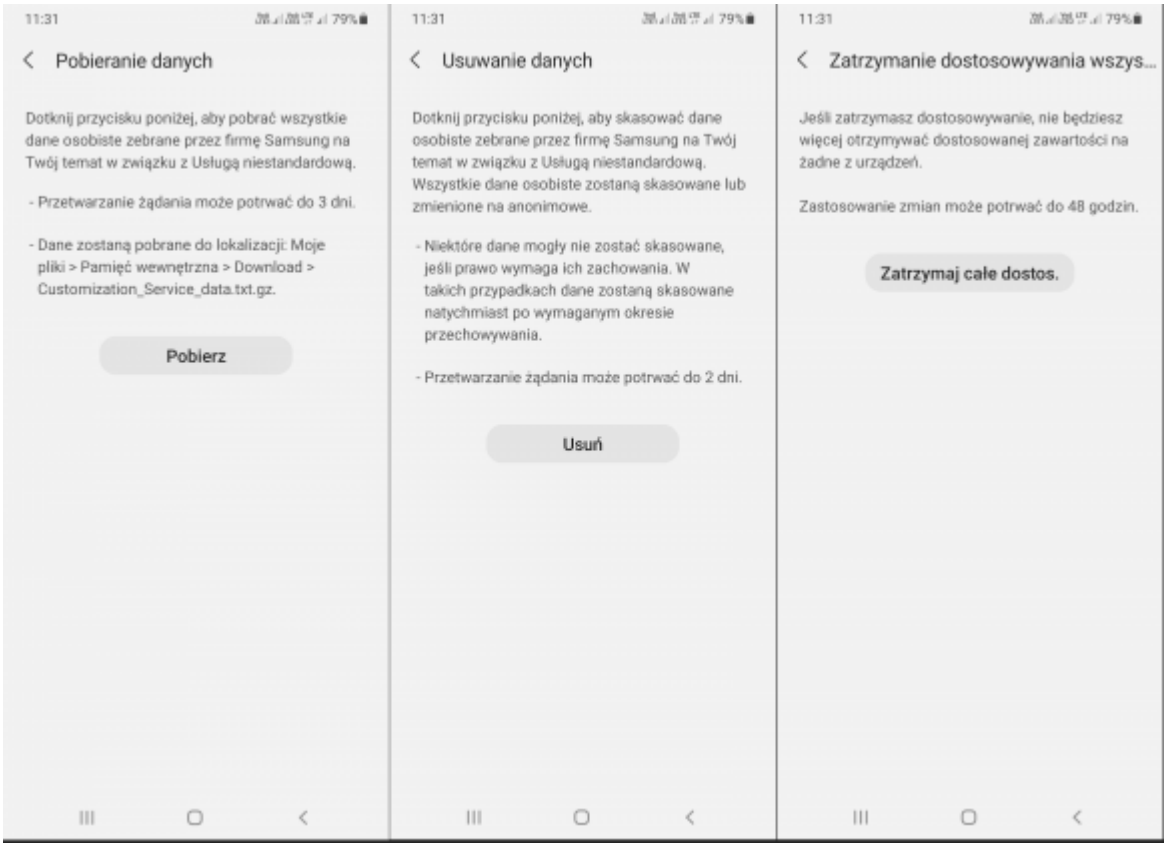
Zgromadzone dane mogą być przekazywane licznym podmiotom, m.in. partnerom biznesowym Samsunga i współpracującym z nim usługodawcom, którzy dokonują napraw, przygotowują spersonalizowane reklamy itp. Informacje o konkretnych użytkownikach mogą być ujawniane „gdy wymaga tego prawo lub gdy jest to niezbędne do ochrony usług firmy Samsung", jak również „na potrzeby organów ścigania, bezpieczeństwa narodowego, walki z terroryzmem lub innych kwestii związanych z bezpieczeństwem publicznym". W polityce prywatności możemy przeczytać, że firma przechowuje dane użytkowników „Wyłącznie przez czas wymagany w celu, w jakim takie informacje zostały zgromadzone lub są przetwarzane, lub dłużej, jeśli wymaga tego jakakolwiek umowa, obowiązujące prawo, bądź w celach statystycznych, z zachowaniem odpowiednich zabezpieczeń". Innymi słowy – nie wiadomo, jak długo i choćby z tego względu warto ograniczyć ilość przekazywanych Samsungowi danych. Dlatego sugerujemy np. nie używać dostarczanej wraz systemem przeglądarki, sugestywnie podpisanej jako „Internet" – lepszy będzie nawet Google Chrome (po włączeniu w ustawieniach „Piaskownicy prywatności"), ale można też pokusić się o zainstalowanie mobilnej wersji Firefoksa albo DuckDuckGo. Nie

zaszkodzi też poszukać alternatywnych rozwiązań dla pozostałych narzędzi oferowanych przez producenta.



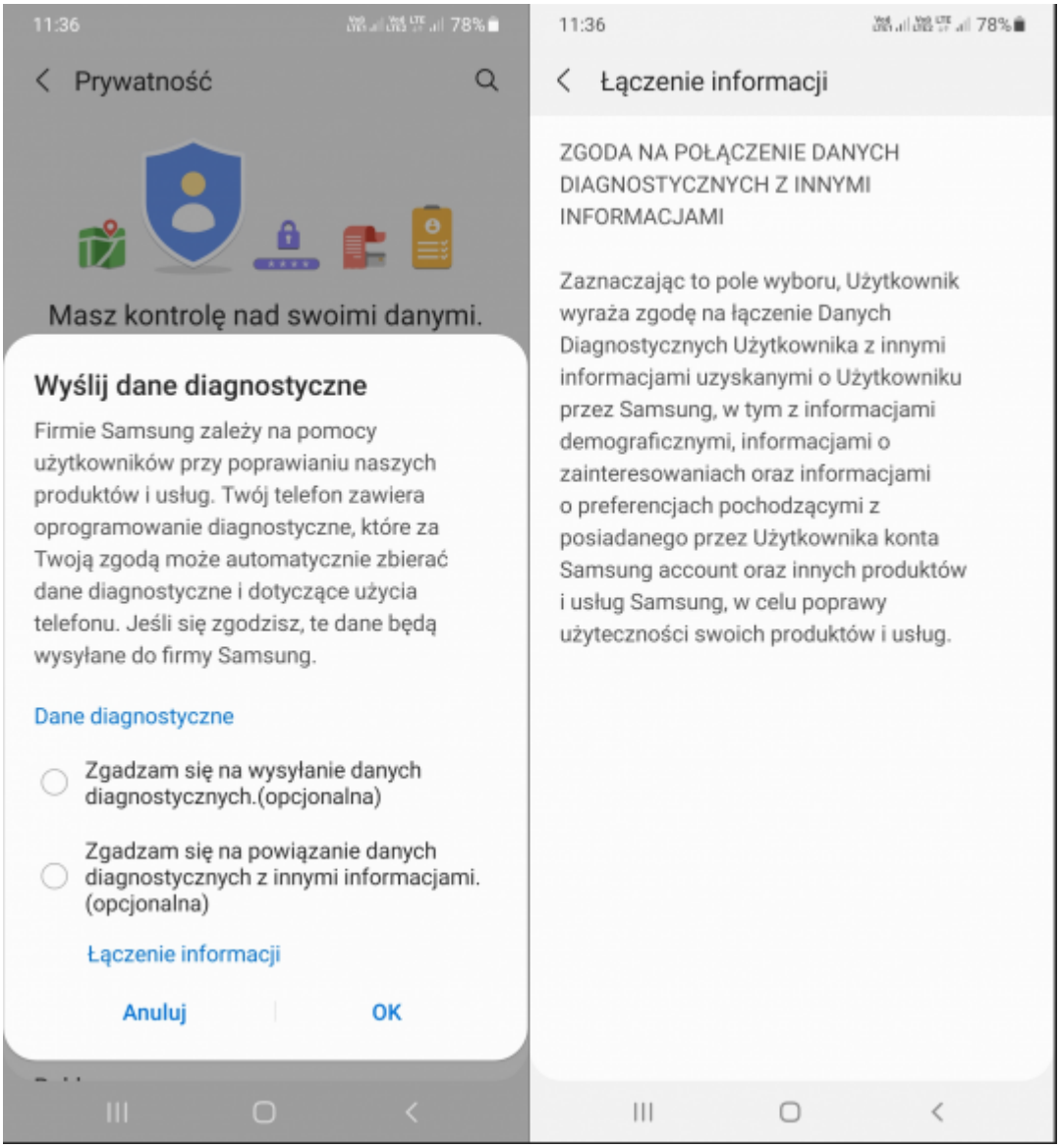
„Usługa niestandardowa” oferowana przez Samsunga

Po wejściu do ustawień telefonu w zakładce „Prywatność” znajdziemy ponadto pozycję „Usługa niestandardowa”, która odpowiada za dostarczanie reklam i innych treści w oparciu o nasze (rzekome) zainteresowania i odwiedzane przez nas miejsca w świecie rzeczywistym. Można ją skonfigurować po zalogowaniu się na założone wcześniej konto w usługach Samsunga. Jeśli opcja „Dostosuj ten telefon” zostanie aktywowana, to w sekcji „Zarządzanie danymi” będziemy mogli określić, czy usługa ma mieć dostęp do naszych połączeń i wiadomości, historii wyszukiwania i przeglądania oraz lokalizacji (ale nie są to jedyne zbierane przez nią informacje, o czym się przekonamy, zaglądając do odrębnej polityki prywatności). W sekcji „Dostosowane aplikacje” możemy z kolei wskazać, które z systemowych aplikacji będą z gromadzonych danych korzystać. Nasza rada? W ogóle tej usługi nie włączać.



Ujarzmianie „Usługi niestandardowej”

Jeśli nieopatrznie zrobiliśmy to wcześniej, możemy skorzystać z opcji „Pobieranie danych” i sprawdzić, czego dowiedział się o nas Samsung. Firma uprzedza, że przetwarzanie żądania może jej zająć nawet 3 dni, a interesujące nas informacje zostaną zapisane w folderze „Download” pod postacią pliku *Customization_Service_data.txt.gz*. Za pomocą opcji „Zatrzym. dostos. wszys. urządz.” możemy zrezygnować z otrzymywania spersonalizowanych treści, nie nastąpi to jednak od razu – zastosowanie zmian może potrwać do 2 dni. Podobnie mają się sprawy z usuwaniem gromadzonych przez usługę danych. Co gorsza, nie wszystkie zostaną skasowane z uwagi na bliżej nieokreślone wymogi prawne, o czym zostaniemy poinformowani przed naciśnięciem przycisku „Usuń”.



Zgoda na wysyłanie do Samsunga danych diagnostycznych

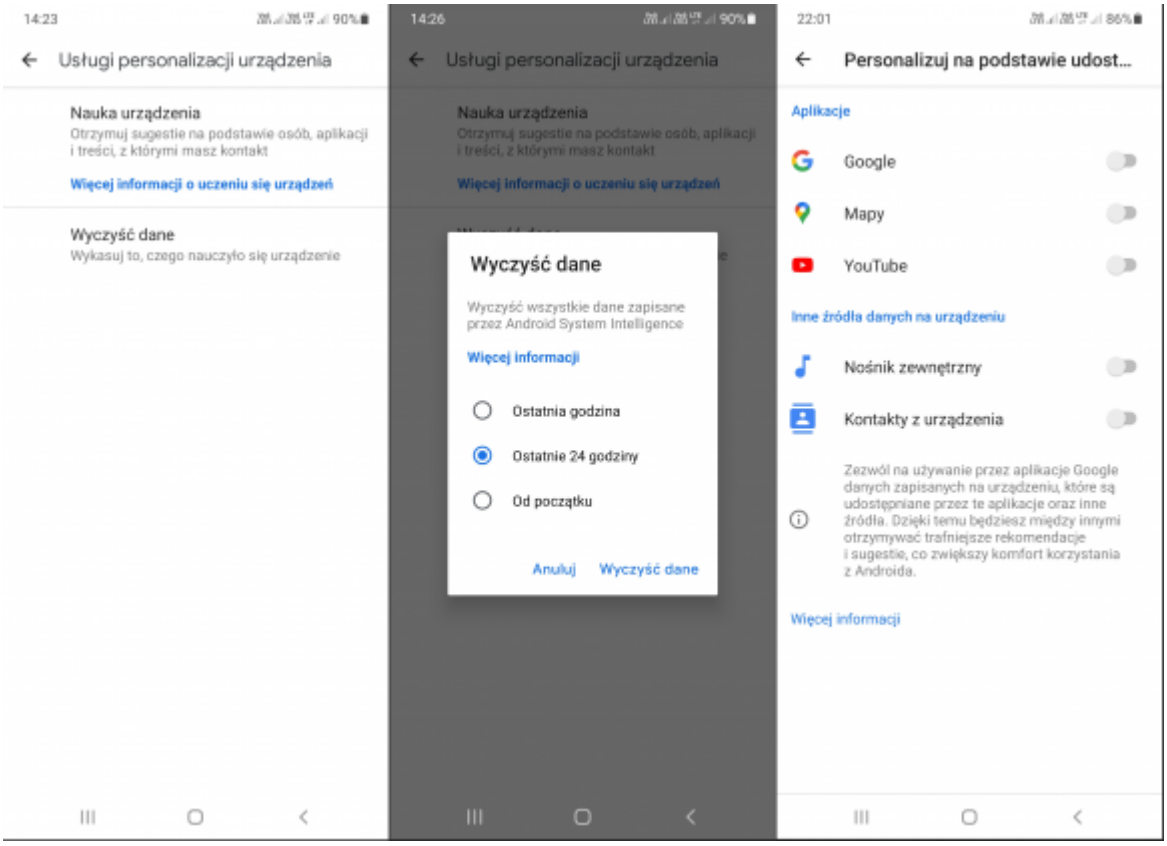
W zakładce „Prywatność” znajdziemy ponadto opcję wysyłania Samsungowi danych diagnostycznych, której również sugerujemy nie aktywować. Klikając w link „Dane diagnostyczne”, dowiemy się, że decyzja o nieprzekazywaniu firmie tego typu informacji nie wpłynie w żaden sposób na funkcjonalność telefonu. Producent zbiera je „w celu doskonalenia jakości produktów i usług oraz monitorowania przypadków i reagowania na przypadki niespodziewanych wyłączeń lub błędów systemu”. Jak widać na powyższym zrzucie ekranu, dane te za zgodą użytkownika mogą zostać powiązane z innymi informacjami o nim, które firma pozyskuje z różnych źródeł. Samsung zakłada, że cykl życia urządzeń przenośnych wynosi dwa lata i zapewnia, że po tym czasie informacje osobiste będą automatycznie usuwane (ale jak wiemy z polityki prywatności, nie brakuje od tej reguły

wyjątków).

Jeśli się zastanawiacie, czy inne firmy produkujące smartfony z Androidem gromadzą mniej danych albo obchodzą się z nimi lepiej, to odpowiedź brzmi „raczej nie”, o czym możecie się przekonać, zaglądając do ich polityk prywatności. Oto kilka przykładowych: Xiaomi, Huawei, Alcatel, Sony.

Ujarzmianie usług Google

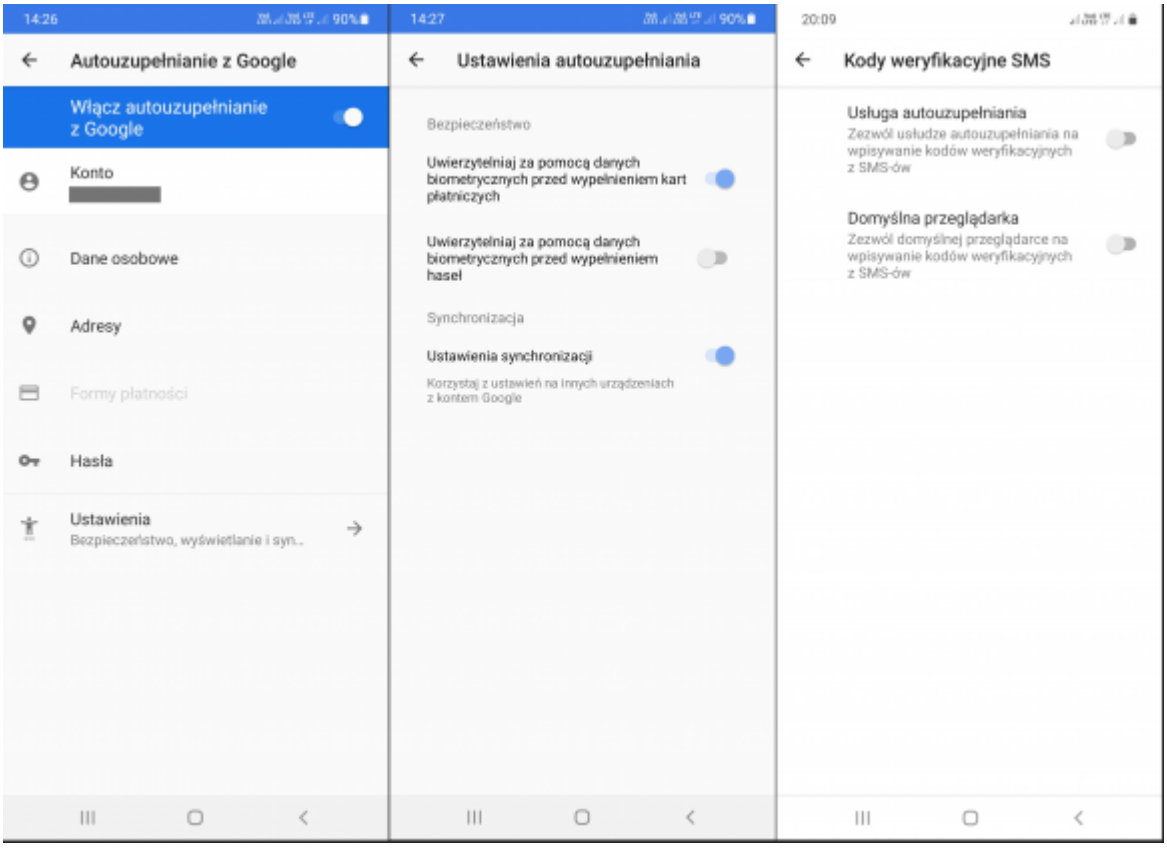
Przegląd ustawień prywatności związanych z usługami Google zaczynamy od możliwości personalizacji urządzenia i akurat w tym przypadku nie chodzi o wyświetlanie reklam, tylko o podpowiadanie użytkownikowi na podstawie jego wcześniejszych działań, co może w danej chwili zrobić. Jeśli np. zaznaczymy jakiś tekst, a Google rozpozna, że jest to nazwa restauracji, to możemy otrzymać sugestię otwarcia aplikacji Mapy i wyznaczenia trasy dojazdu. W zakładce „Prywatność” po wybraniu „Usług personalizacji urządzenia” możemy uzyskać więcej informacji na temat tej funkcji, a także usunąć zgromadzone dotychczas dane. W Androidzie 12 omawiana funkcja kryje się pod nazwą „Android System Intelligence” i pozwala dodatkowo włączyć inteligentne podpowiedzi w pasku sugestii klawiatury. W obu przypadkach, jeśli chcemy coś skonfigurować (czyli wskazać lub wykluczyć jakieś źródła danych), musimy się udać do zakładki „Google” i wybrać opcję „Personalizuj na podstawie udostępnionych danych”.



Usługi personalizacji urządzenia

Kolejna warta uwagi pozycja w zakładce „Prywatność” to „Usługa autouzupełniania Google” umożliwiająca automatyczne wpisywanie danych do formularzy, co jest – i owszem – wygodne, ale dostarcza producentowi Androida sporo wrażliwych informacji o użytkowniku. Jeśli włączymy tę funkcję, to po kliknięciu w „Dane osobowe” przeniesiemy się do sekcji zarządzania osobistymi informacjami na koncie Google, „Adresy” pozwolą nam ustawić adres domowy i służbowy w aplikacji Mapy, „Formy płatności” będą aktywne tylko po ich wcześniejszym skonfigurowaniu (w sekcji „Google” » „Ustawienia aplikacji Google” » „Google Pay”), a „Hasła” dadzą dostęp do wbudowanego menedżera haseł. Wybierając „Ustawienia”, będziemy mogli określić, czy chcemy uwierzytelniać się za pomocą biometrii przed wypełnieniem danych kart płatniczych i/lub haseł, a także zezwolić na synchronizację ustawień tej usługi na innych urządzeniach. Jeśli natomiast przejdziemy do sekcji „Autouzupełnianie” w zakładce „Google”, to znajdziemy tam m.in. opcję „Kody weryfikacyjne SMS”. Ze względów bezpieczeństwa nie powinniśmy zezwalać na wpisywanie kodów weryfikacyjnych z SMS-ów ani usłudze autouzupełniania, ani

domyślnej przeglądarce.

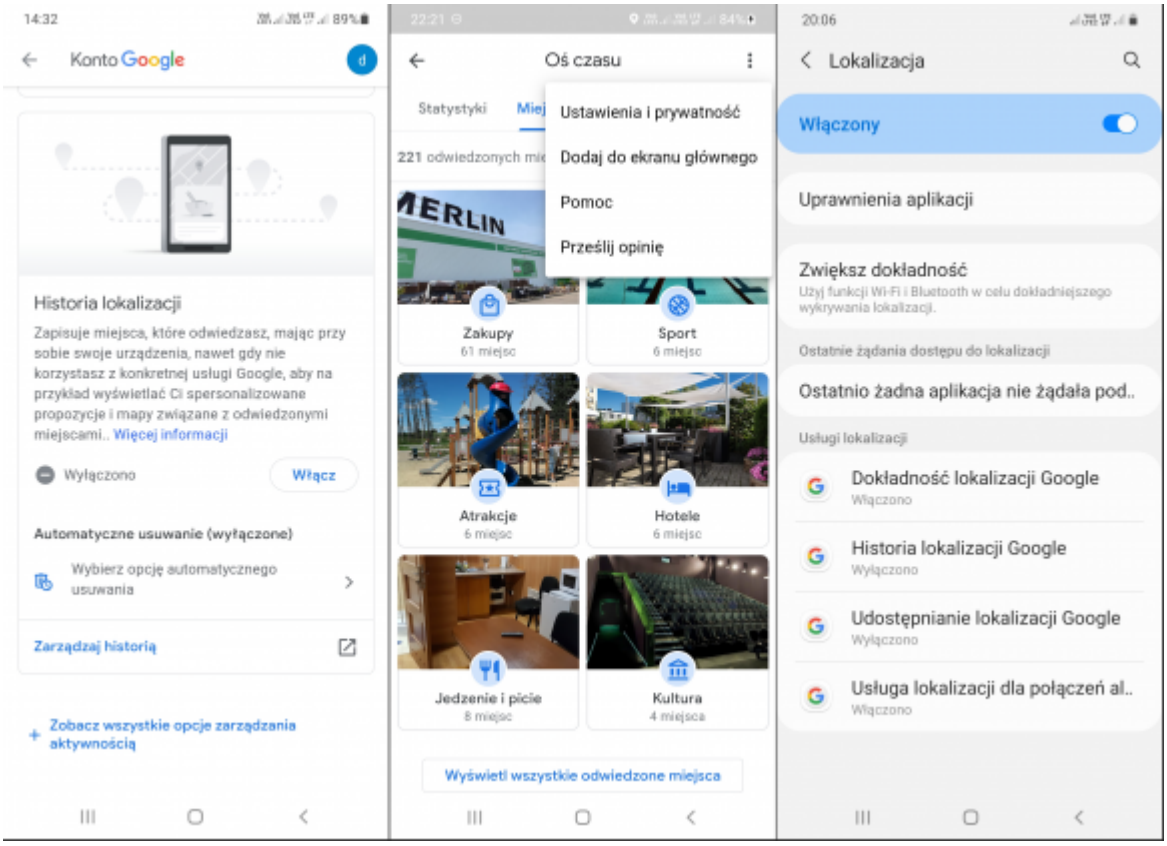


Ustawienia autouzupełniania

Przejdźmy teraz w zakładce „Prywatność” do sekcji „Historia lokalizacji Google”. Możemy ją od razu wyłączyć, lepszym pomysłem będzie jednak skorzystanie z opcji „Zarządzaj historią” i przejrzenie zapisanych przez firmę informacji o naszym przemieszczaniu się w świecie rzeczywistym. Klikając w trzy kropki widoczne po prawej stronie ekranu i wybierając „Ustawienia i prywatność”, uzyskamy m.in. możliwość usunięcia całej historii lokalizacji lub pewnego jej zakresu, a także skonfigurowania automatycznego usuwania gromadzonych danych – możemy w ten sposób na bieżąco kasować aktywność starszą niż 3, 18 lub 36 miesięcy.

Dodatkowe opcje znajdziemy w odrębnej zakładce „Lokalizacja”, dostępnej bezpośrednio z głównego menu ustawień smartfona. W sekcji „Uprawnienia aplikacji” możemy zobaczyć, jakim aplikacjom przyznaliśmy ciągły dostęp do danych lokalizacyjnych, jakie mają do nich dostęp tylko podczas używania i jakim nie daliśmy dostępu, choć o niego prosiły. W

przypadku pomyłki istnieje oczywiście możliwość skorygowania wcześniejszych wyborów. Standardowo lokalizacja urządzenia jest wykrywana za pomocą GPS, możemy jednak aplikacjom zezwolić na korzystanie z Wi-Fi i Bluetootha w celu dokładniejszego jej określania (co może się przydać, jeśli na fali sentymentu nadal gramy w Pokemon Go albo skonfigurowaliśmy zaufane miejsca w funkcji Smart Lock – zob. *Biometria i inne sposoby ochrony Androida przed niepowołanym dostępem*). Udostępniając swoją lokalizację innym osobom, powinniśmy pamiętać, że mogą się one dowiedzieć nie tylko, gdzie jesteśmy obecnie, ale również gdzie byliśmy przedtem, w jaki sposób się przemieszczamy (jedziemy czy idziemy), jaki jest stan naszego urządzenia, w tym np. stopień naładowania baterii i parę innych rzeczy – dlatego sugerujemy korzystać z tej opcji z rozwagą. Warto natomiast aktywować „Usługę lokalizacji dla połączeń alarmowych (ELS)". Jak tłumaczy producent systemu: „Gdy zadzwonisz lub napiszesz SMS-a na numer alarmowy, może zostać wysłana również lokalizacja Twojego telefonu, aby ratownicy mogli szybko Cię odnaleźć. Numer alarmowy w Stanach Zjednoczonych to 911, a w Europie 112".

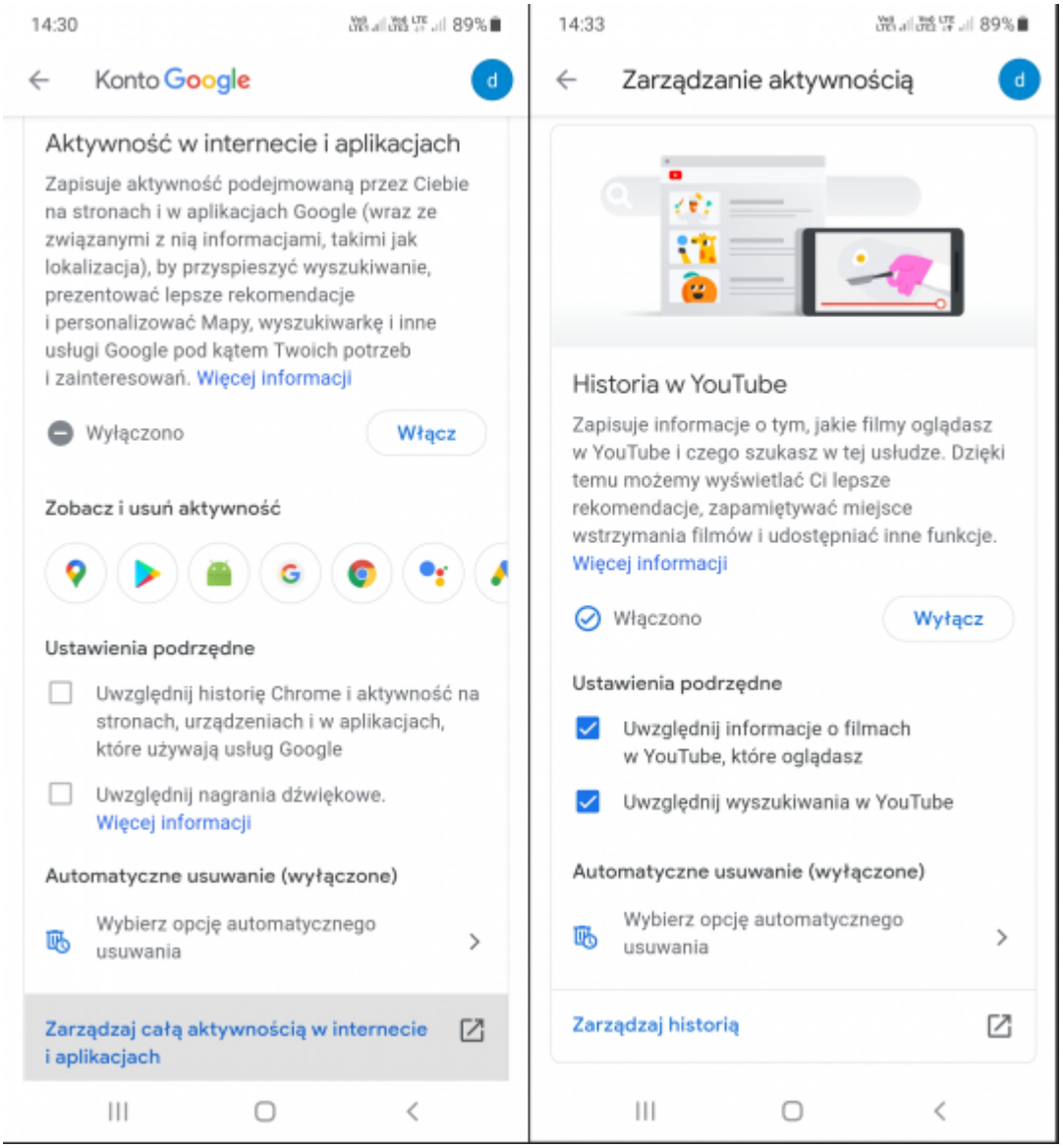


Zarządzanie lokalizacją

Wróćmy jednak do zakładki „Prywatność” i wybierzmy „Zarządzanie aktywnością”. Zobaczymy cztery sekcje: „Aktywność w internecie i aplikacjach”, ponownie (omówioną już) „Historię lokalizacji”, „Historię w YouTube” i „Personalizację reklam”.

Decydując się na zapisywanie naszej aktywności w internecie i aplikacjach, dowiemy się, że gromadzone dane „pomagają personalizować usługi Google, np. pozwalają szybciej wyszukiwać informacje oraz zwiększają trafność rekomendacji i reklam – zarówno w usługach Google, jak i innych firm”. Wniosek? Nic złego się nie stanie, jeśli wyłączymy tę funkcję. Jeśli tego nie zrobimy, możemy ograniczyć ilość zapisywanych informacji poprzez nieuwzględnianie historii przeglądarki Chrome i nagrań dźwiękowych generowanych podczas interakcji z wyszukiwarką Google, Asystentem i Mapami. Klikając w link „Więcej informacji”, przeczytamy, że ustawienie to „nie ma wpływu na dane dźwiękowe zapisane na Twoim urządzeniu i w innych usługach Google ani na sposób, w jaki Google przetwarza, transkrybuje i wykorzystuje do nauki Twoje dane w czasie rzeczywistym”. Tak jak w przypadku historii

lokalizacji, możemy skonfigurować automatyczne usuwanie zebranych danych. Wybierając „Zarządzaj całą aktywnością w internecie i aplikacjach”, otrzymamy także możliwość wyszukiwania i filtrowania zapisanych treści według dat i usług. Podobnie wygląda zarządzanie historią serwisu YouTube.

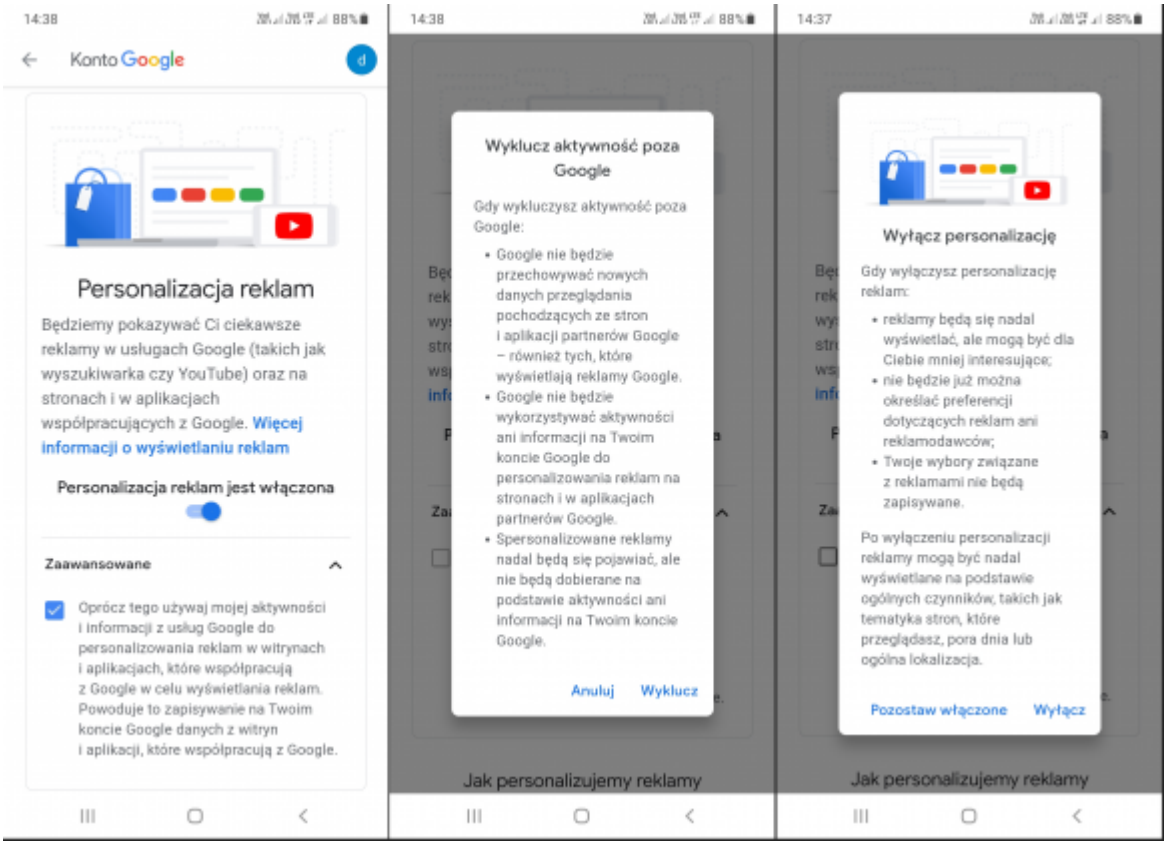


Zarządzanie aktywnością

Inaczej mają się sprawy z funkcją „Personalizacja reklam”. Jeśli jest ona włączona, to w sekcji „Jak personalizujemy reklamy” zobaczymy, na podstawie jakich danych osobowych Google dopasowuje do nas przekaz reklamodawców (przykładowe pozycje: „45-54 lata”, „Mężczyzna”, „Język: polski i jeszcze 1”). Każdą z uwzględnionych informacji możemy zaktualizować, a w przypadku profilowania na podstawie naszych zainteresowań – wyłączać te, z którymi się nie utożsamiamy i przywracać

wyłączone przez pomyłkę. W sekcji „Reklamy o charakterze kontrowersyjnym w YouTube” możemy ograniczyć wyświetlanie reklam dotyczących alkoholu i hazardu, a od pewnego czasu także randek, ciąży i rodzicielstwa czy nawet odchudzania. Na dole widnieje link „Twoje dane i reklamy”, pod którym znajduje się zapewnienie Google, że nigdy nie sprzedaje danych osobowych i nie używa informacji poufnych do personalizowania reklam. Sami musicie zadecydować, czy w to wierzycie. Bloomberg donosi, że z 68 mld dolarów całkowitych przychodów firmy w kwartale zakończonym 31 marca br. około 54 mld pochodziło z usług reklamowych.

Aby zapewnić sobie więcej prywatności, możemy usunąć zaznaczenie jedynej, niezbyt jasno opisanej opcji w zakładce „Zaawansowane” – dzięki temu Google nie będzie używać naszych danych do personalizowania reklam wyświetlanych na stronach i w aplikacjach firm trzecich, które z nim współpracują. Nie będzie też zapisywać informacji o naszych działaniach na stronach i w aplikacjach należących do zewnętrznych usługodawców. Jeszcze lepszym pomysłem jest całkowite wyłączenie personalizacji. Twórcy Androida uprzedzają, że reklamy nadal będą się nam wyświetlać, ale mogą być mniej interesujące – niewielka strata. Potwierdzając swój wybór, zobaczymy komunikat o możliwości wyłączenia personalizacji reklam Google wyświetlanych bez logowania oraz reklam z ponad 100 innych internetowych sieci reklamowych – da się tego dokonać w serwisie Your Online Choices (chociaż nie jest to rozwiązanie bez wad, bo opiera się na ciasteczkach).

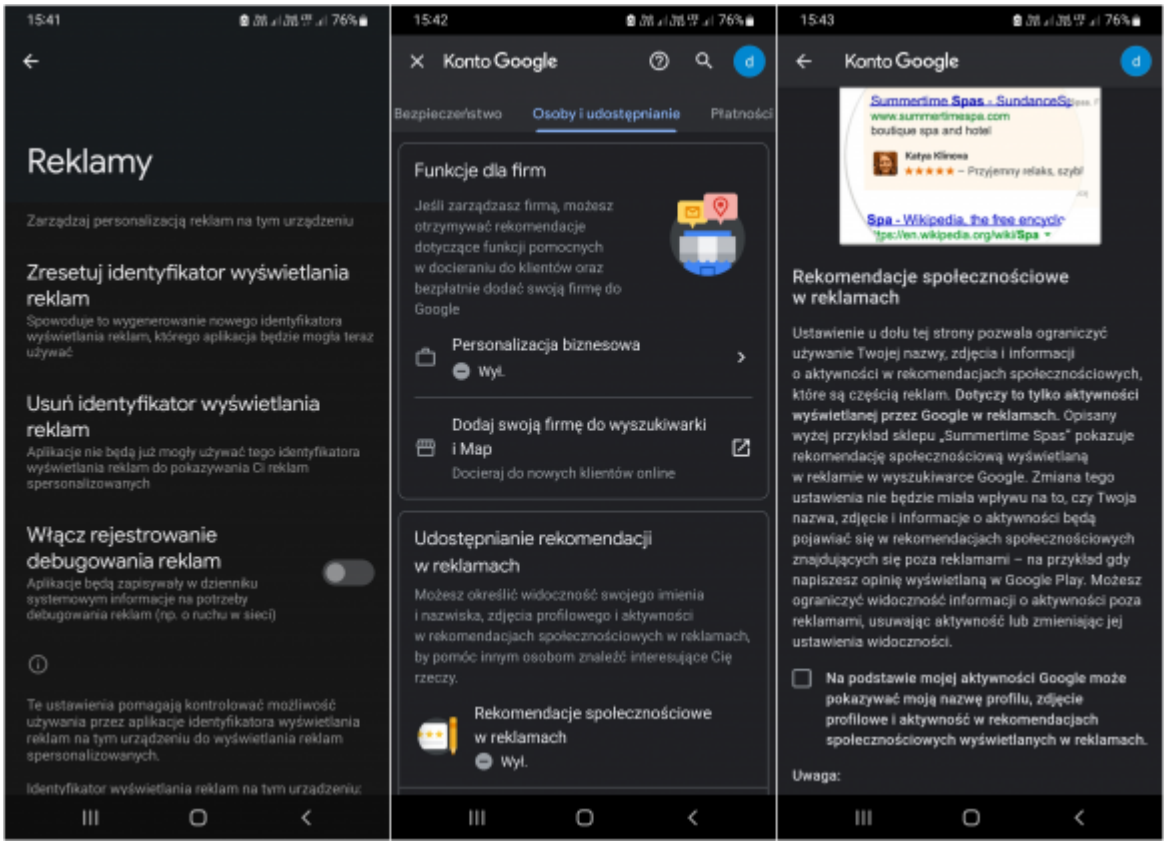


Personalizacja reklam

W zakładce „Prywatność” znajdziemy też odrębną sekcję „Reklamy”. W to samo miejsce trafimy, wybierając opcję o identycznej nazwie po wejściu z głównego menu ustawień do zakładki „Google” (czemu służy takie dublowanie ścieżek, nie wiadomo – może zamotaniu niedoświadczonego użytkownika, który dzięki temu coś przeoczy). W sekcji tej możemy zresetować unikalny identyfikator, który pozwala usługodawcom śledzić nasze zwyczaje i zainteresowania w celu lepszego dopasowania prezentowanych nam reklam. Identyfikator ten możemy również usunąć bez zastępowania go nowym. W Androidzie 12 stosowną opcję znajdziemy bez większych problemów, w starszych wersjach systemu kryje się ona natomiast pod nieco mylącą nazwą „Rezygnacja z personalizacji reklam”, którą dla odmiany trzeba włączyć.

Innej ukrytej funkcji musimy poszukać, wciskając w zakładce „Google” przycisk „Zarządzaj kontem Google”. Z górnego menu wybieramy „Osoby i udostępnianie”, przechodzimy do sekcji „Udostępnianie rekomendacji w reklamach” i klikamy w link „Zarządzaj rekomendacjami społecznościowymi”. Zobaczymy ścianę

tekstu wyjaśniającą, czym są wspomniane rekomendacje – w skrócie chodzi o możliwość wykorzystania w celach reklamowych naszej nazwy użytkownika, zdjęcia i informacji o aktywności (np. dodanej przez nas opinii o jakiejś restauracji). Aby temu zapobiec, trzeba zjechać na dół strony i usunąć zaznaczenie znajdującego się tam pola wyboru.

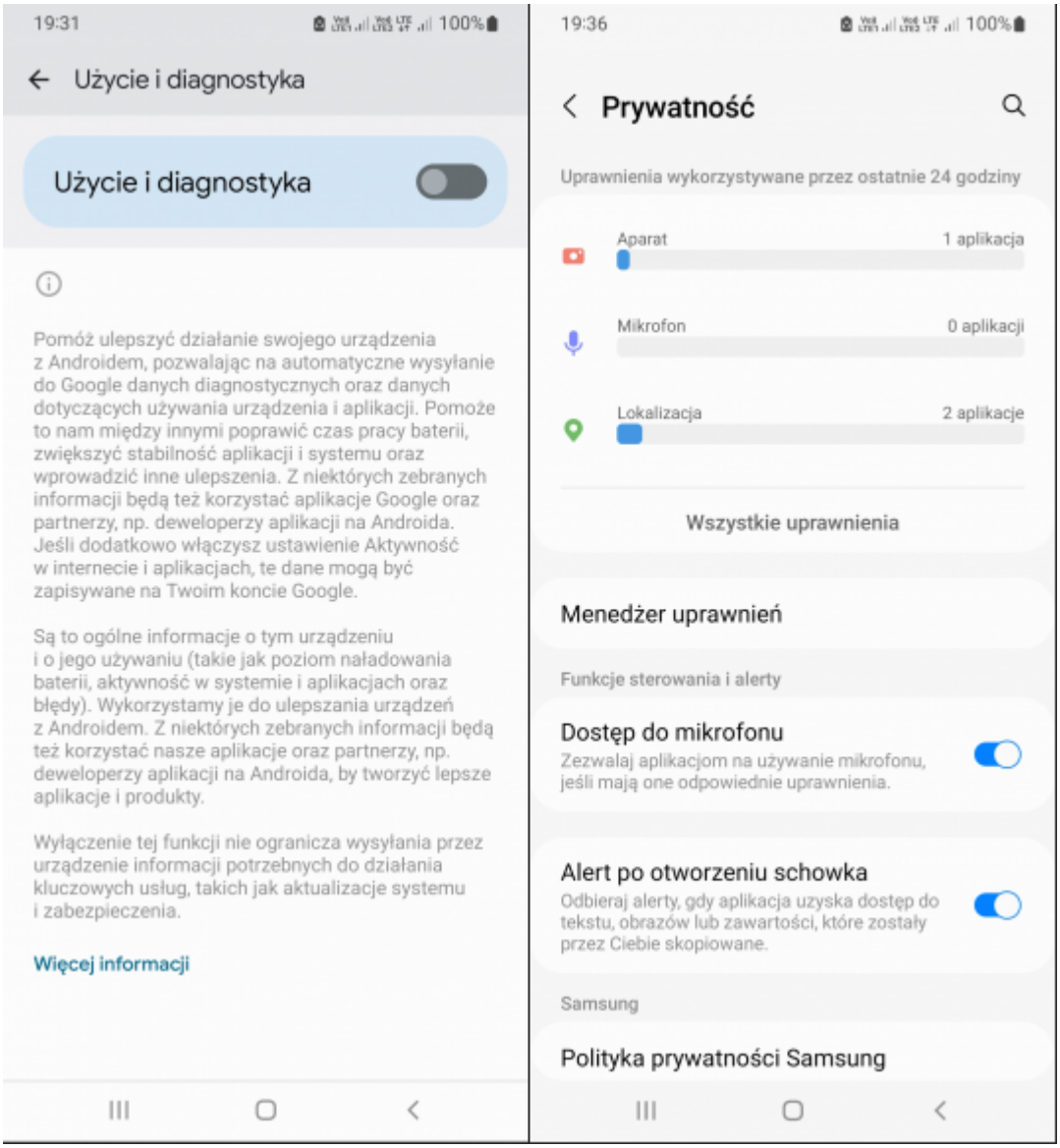


Reklamy i rekomendacje społecznościowe

Więcej sugestii dotyczących zarządzania kontem Google można znaleźć w naszych wcześniejszych artykułach z cyklu Podstawy Bezpieczeństwa: *Jak zadbać o swoją prywatność w usługach Google* oraz *Jak zadbać o swoje bezpieczeństwo w usługach Google*.

Ostatnią wartą uwagi sekcją w zakładce „Prywatność” jest „Użycie i diagnostyka”, która po włączeniu przesyła producentowi systemu informacje o jego działaniu i ewentualnych problemach. Ze strony pomocy technicznej Google możemy się dowiedzieć, że firmę interesują również takie dane, jak częstotliwość używania aplikacji, poziom naładowania baterii oraz jakość i czas trwania połączeń sieciowych. Są one

zapisywane na koncie użytkownika, co oznacza, że da się je przejrzeć i usunąć za pośrednictwem strony Moja aktywność. Przesyłanie tych informacji nie jest konieczne do poprawnego funkcjonowania Androida, możemy więc tę funkcję zdezaktywować.



Wysyłanie danych diagnostycznych i inne opcje

Spośród nowych opcji, które dodano w Androidzie 12, warto wymienić możliwość cofnięcia wszystkim aplikacjom dostępu do mikrofonu (wystarczy posłużyć się jednym suwakiem) oraz alerty po otworzeniu schowka. W kolejnej wersji Androida ma się pojawić także automatyczne usuwanie historii schowka, dzięki czemu aplikacje zostaną prewencyjnie odcięte od wcześniej skopiowanych, nieprzeznaczonych dla nich informacji. Wchodząc do zakładki „Prywatność”, możemy teraz zobaczyć statystyki wykorzystania aparatu, mikrofonu i lokalizacji w ciągu

ostatnich 24 godzin. Kliknięcie w którąkolwiek z tych funkcji umożliwia zapoznanie się z dokładną historią jej użycia. W Androidzie 13 liczba aplikacji wymagających dostępu do lokalizacji może ulec zmniejszeniu – nie trzeba będzie np. przyznawać tego uprawnienia, aby włączyć skanowanie Wi-Fi.

Na konferencji Google I/O, która odbyła się w maju, firma poinformowała o dostępności „trzynastki" w wersji beta 2, którą wyposażono w wymienione wyżej i sporo innych nowości. Można ją przetestować na smartfonach kilku różnych producentów, ale Samsung się do nich nie zalicza. Cóż, poczekamy… zwłaszcza że Android 12 ledwo zaczął zdobywać popularność. Według statystyk dostępnych na stronie StatCounter na razie używa go tylko 11,77% posiadaczy telefonów z tym systemem, a w Polsce jeszcze mniej, bo 9,78%. Niekwestionowanym liderem pozostaje „jedenastka", która na szczęście przykłada do prywatności użytkowników większą wagę niż poprzedniczki.

Dla zachowania pełnej przejrzystości: Patronem cyklu jest Aruba Cloud. Za opracowanie i opublikowanie tego artykułu pobieramy wynagrodzenie.

Źródło