

Nowe wytyczne dot. marketingu RODO w praktyce

W TYM WYDANIU:

- 1. Marketing bezpośredni a RODO – wytyczne belgijskiego urzędu ochrony danych osobowych a obecna praktyka **1**
- Regulacje w zakresie marketingu bezpośredniego **3**
- Interes administratora jako podstawa przetwarzania **6**
- Czy wytyczne belgijskiego UODO są zgodne z aktualnym stanowiskiem polskich organów nadzoru? **8**
- 2. Jak zidentyfikować, dopuścić do korzystania z zasobów i rozliczyć działalność użytkownika w systemach przetwarzania informacji? **11**
- Kryteria identyfikacji **12**
- Rozliczalność procesów **19**



Olga Ograbisz

Information Security & Data Protection Expert

Marketing bezpośredni a RODO – wytyczne belgijskiego urzędu ochrony danych osobowych a obecna praktyka

Marketing bezpośredni stanowi jeden z ważniejszych i najbardziej rozpowszechnionych celów przetwarzania danych osobowych. Choć żaden z krajowych przepisów ani przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „RODO”) nie definiuje wprost pojęcia marketingu bezpośredniego, to występuje ono wielokrotnie w motywach RODO czy ustawy prawo komunikacji elektronicznej (ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej) i weszło też na stałe do obrotu gospodarczego.

Co więcej, ze względu na charakter działań podejmowanych w ramach marketingu bezpośredniego budzi on niezmiennie wiele kontrowersji i znaków zapytania – przede wszystkim dotyczących tego, jakie działania uznamy za zgodne z prawem, a jakie te prawo naginają lub łamią? Z tematem ostatnio zmierzył się belgijski organ nadzoru (odpowiednik naszego Urzędu Ochrony Danych Osobowych), który 10 marca 2025 r. opublikował draft wytycznych dla marketingu

bezpośredniego. Konsultacje zaproponowanego podejścia będą trwały do 10 maja 2025 r.

Zacznijmy od podstawy, czyli definicji i jej składowych

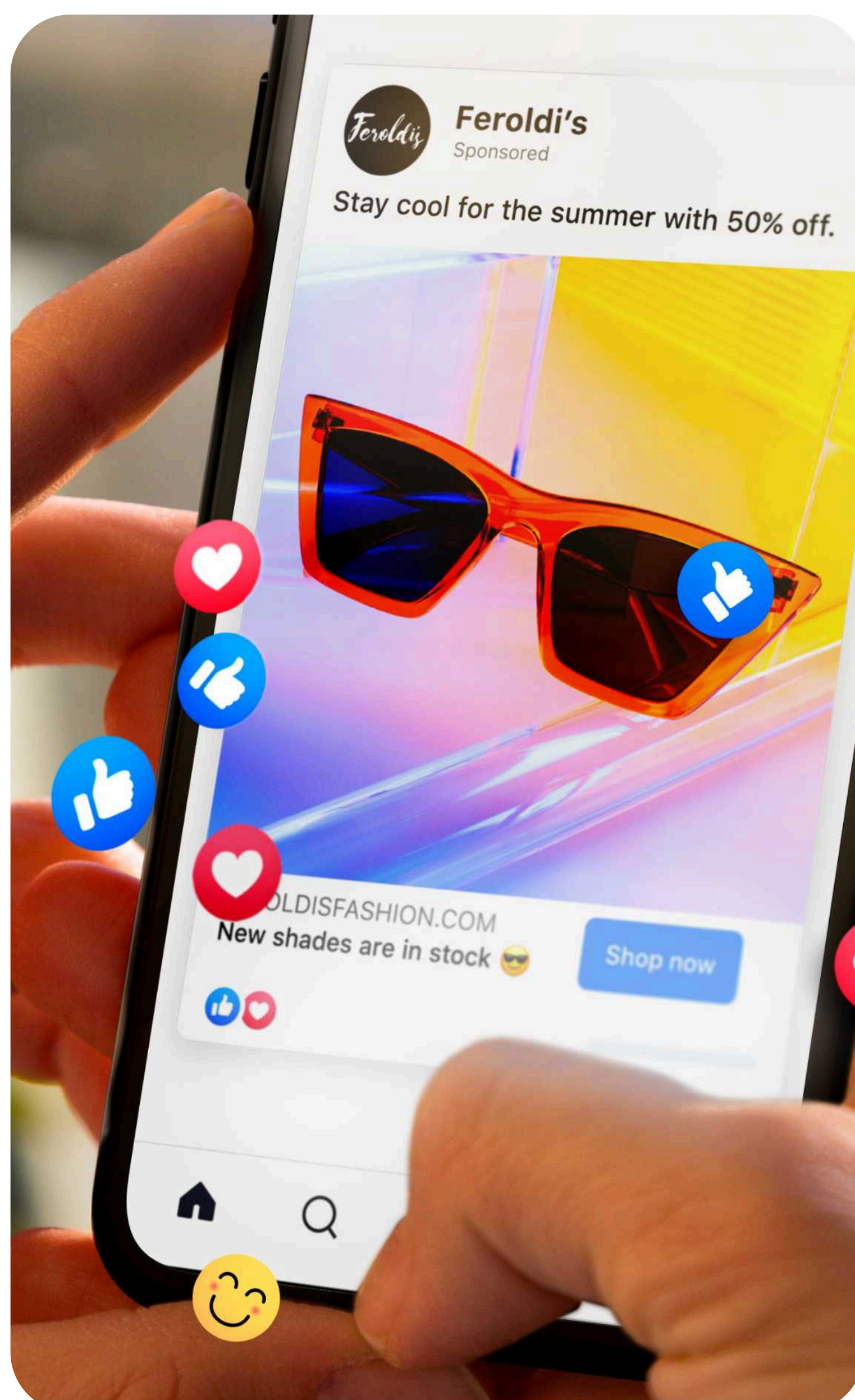
Marketing bezpośredni definiowany jest w różnoraki sposób. Najprościej można powiedzieć, że **pod tym pojęciem rozumiemy "wszelkie działania skutkujące bezpośrednim przekazywaniem jednej lub większej liczbie zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych komunikatów o treści promocyjnej"**. Może on przybrać formę reklamy i promocji, w ramach której materiały o takiej zawartości kierowane są bezpośrednio przy użyciu usług łączności elektronicznej – takich jak m.in. telefon, e-mail, sms, mms.

Analizując definicję marketingu bezpośredniego i to, czym on faktycznie jest, warto uwzględnić stanowisko wspomnianego powyżej belgijskiego organu, który precyzuje zakres definicji w następujący sposób:

- marketing bezpośredni odnosi się nie tylko do komunikacji jako takiej, ale także do wszystkich działań (w tym wcześniejszego przetwarzania danych) prowadzonych na potrzeby komunikacji – obejmuje to na przykład przetwarzanie danych w celu dostosowania cen, profilowanie klientów w celu wysyłania ukierunkowanych wiadomości, a także działania brokerów danych, którzy zajmują się marketingiem danych osobowych w celu wysyłania komunikatów promocyjnych;
- zakres definicji obejmuje zarówno komunikaty marketingu bezpośredniego zamówione, jak i niezamówione – to, czy odbiorca prosił o komunikat, nie ma znaczenia dla uznania go za marketing bezpośredni, choć może mieć znaczenie w kontekście dyrektywy o prywatności i łączności elektronicznej;
- działalność w zakresie marketingu bezpośredniego zakłada istnienie przetwarzania danych osobowych – komunikat musi być skierowany do co najmniej jednej zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, co wiąże się z przetwarzaniem jej danych osobowych, takich jak numer telefonu, adres pocztowy, adres e-mail czy adres IP. Komunikacja, która nie wiąże się z przetwarzaniem danych osobowych, jest wyłączona z zakresu definicji;
- tożsamość osoby fizycznej lub prawnej, której usługi, towary lub działania są promowane w komunikacie marketingu bezpośredniego, nie ma znaczenia - komunikaty mogą być wysyłane przez podmioty komercyjne, organizacje non-profit, władze publiczne czy partie polityczne;
- pojęcie treści promocyjnych powinno być rozumiane w najszerszym znaczeniu (na przykład o charakterze komercyjnym lub niekomercyjnym, nie wyłączając treści mieszanych łączących marketing bezpośredni z treściami czysto informacyjnymi) – promocja może dotyczyć produktów, usług, pomysłów, osób, wydarzeń, a komunikat może łączyć treści promocyjne z innymi treściami. Wyjątkiem jest promocja prowadzona przez organy publiczne działające ściśle w ramach swoich obowiązków

prawnych lub misji służby publicznej w odniesieniu do usług, za które tylko one są odpowiedzialne, chyba że promują również usługi lub produkty prywatnych usługodawców. Z definicji wyłączone są również kontakty w celu badań rynkowych, badań satysfakcji czy sondaży opinii publicznej, o ile komunikacja ogranicza się do tego celu i nie służy również sprzedaży lub promocji, ani nie umożliwia wykorzystania danych do celów marketingowych;

- środki wykorzystywane do wysyłania komunikatów marketingu bezpośredniego nie są istotne – marketing bezpośredni może przybierać różne formy, zarówno elektroniczne (np. e-mail, SMS, reklamy online targetowane na podstawie danych osobowych), jak i nieelektroniczne (np. przesyłki pocztowe, sprzedaż obwoźna).



CELE MARKETINGU BEZPOŚREDNIEGO

- 🔗 informowanie klientów o nowych produktach i usługach
- 🔗 inicjowanie sprzedaży produktów i/lub usług
- 🔗 profilowanie klientów
- 🔗 umożliwianie stronom trzecim wykorzystywania danych klientów do określonych celów, takich jak sporządzanie profili konsumentów lub wyborców
- 🔗 proponowanie spersonalizowanych ofert, na przykład z okazji urodzin klientów
- 🔗 informowanie klientów o akcjach promocyjnych
- 🔗 promowanie wizerunku marki wśród ogółu społeczeństwa
- 🔗 zapraszanie klientów lub potencjalnych klientów na wydarzenia w celu promowania organizacji
- 🔗 przekazywanie klientom ukierunkowanych ofert, które mogą odpowiadać ich zainteresowaniom
- 🔗 pozyskiwanie nowych klientów, subskrybentów lub podmiotów stowarzyszonych

Regulacje prawne w zakresie marketingu bezpośredniego

W polskim prawie działalność w obszarze marketingu bezpośredniego regulowana jest przez RODO w kontekście ochrony danych osobowych oraz od 12 lipca 2024 r. przez ustawę **Prawo komunikacji elektronicznej (PKE)**, która zastąpiła ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną oraz ustawę z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. Podobny model funkcjonuje również w pozostałych państwach członkowskich Unii Europejskiej.

Belgijski organ nadzoru w wielu aspektach wspomina także o Dyrektywie o prywatności i łączności elektronicznej i jej interakcji z RODO. Dyrektywa o prywatności i łączności elektronicznej, znana również jako ePrivacy Directive (2002/58/WE), to unijne przepisy regulujące ochronę prywatności w komunikacji elektronicznej. Jest uzupełnieniem ogólnego Rozporządzenia o Ochronie Danych Osobowych (RODO) i koncentruje się na takich kwestiach jak:

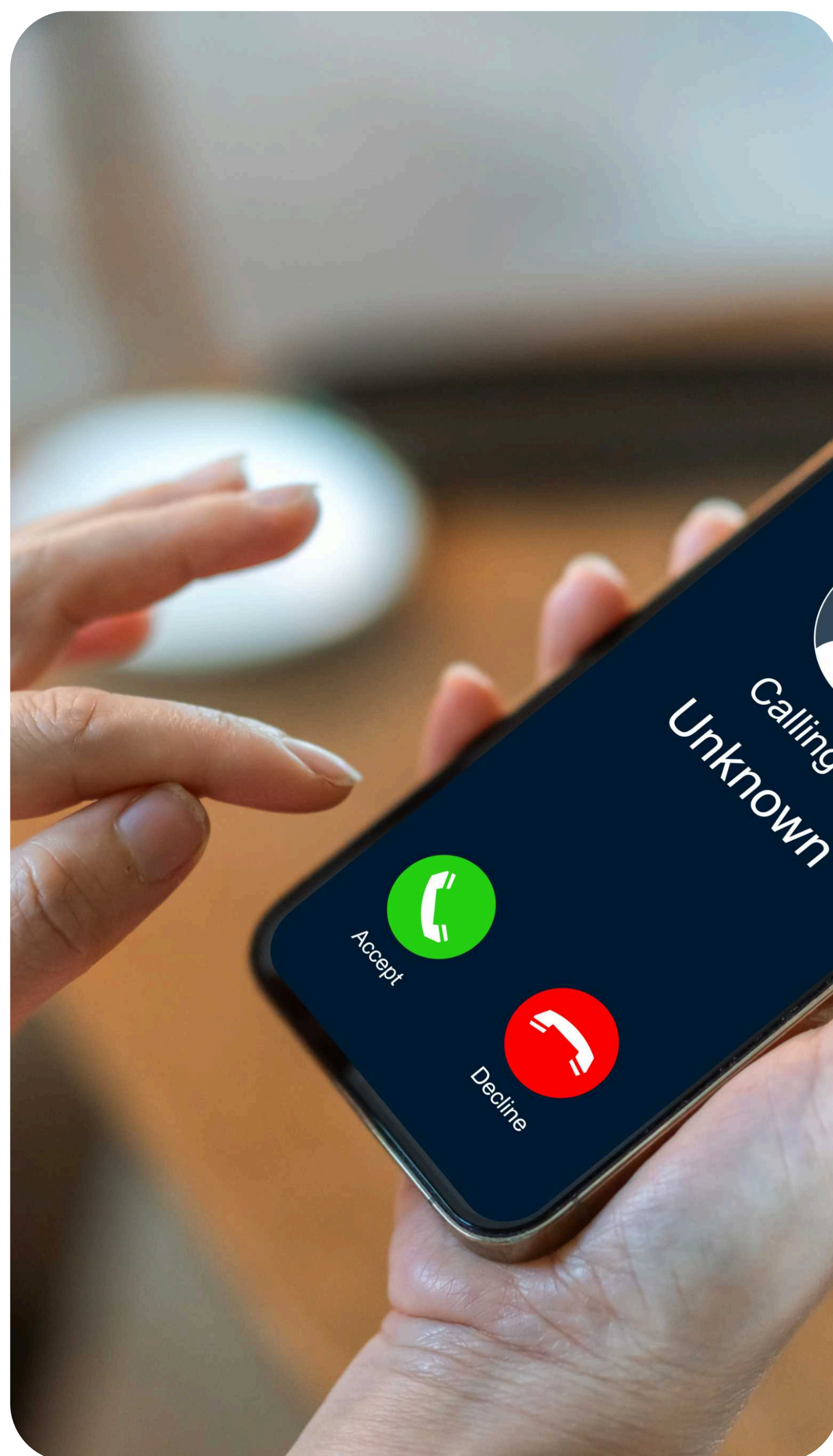
- poufność komunikacji elektronicznej – zapewnia, że rozmowy, e-maile i inne formy komunikacji są chronione przed nieuprawnionym dostępem;
- pliki cookies i technologie śledzące – wymaga uzyskania zgody użytkowników na przechowywanie i dostęp do plików cookie (z pewnymi wyjątkami, np. dla plików niezbędnych do działania strony);
- SPAM i marketing bezpośredni – reguluje zasady wysyłania e-maili marketingowych i połączeń telemarketingowych;
- bezpieczeństwo sieci i usług – nakłada obowiązki na dostawców usług komunikacyjnych w zakresie ochrony danych użytkowników.

Dyrektywa o prywatności i łączności elektronicznej pojawia się w wytycznych belgijskiego organu nadzorczego jako kluczowy akt prawny regulujący elektroniczne formy marketingu bezpośredniego, mający specyficzne wymagania dotyczące zgody i interreagujący z przepisami RODO w tym obszarze. Dokument szczegółowo analizuje te interakcje oraz ich implementację w prawie belgijskim.

Zasady stosowania marketingu bezpośredniego

Zgodnie ze stanowiskiem belgijskiego organu, aby działania związane z marketingiem bezpośrednim można było uznać za zgodne z prawem konieczne jest:

- **spełnienie obowiązku informacyjnego:** dostawca usług komunikacji elektronicznej jest zobowiązany poinformować użytkownika końcowego lub abonenta o zakresie i celu przetwarzania danych transmisyjnych oraz innych danych ich dotyczących do celów marketingu usług komunikacji elektronicznej,
- **uzyskanie uprzedniej zgody** abonenta lub użytkownika końcowego na wykorzystanie automatycznych systemów wywołujących, faksów, telefonu lub poczty elektronicznej do przesyłania informacji handlowej, w tym marketingu bezpośredniego;
- **zapewnienie możliwości sprawnego wycofania udzielonej zgody** w tak prosty sposób jak ją wyraził i za pomocą analogicznych środków/narzędzi;
- **zapewnienie prawa do wniesienia sprzeciwu** wobec przetwarzania danych osobowych w celach marketingu bezpośredniego a także zapewnienie przejrzystej informacji dotyczącej prawa do sprzeciwu - musi zostać ono wyraźnie podane do wiadomości osobie, której dane dotyczą, oraz powinno być przedstawione jasno i oddzielnie od wszelkich innych informacji



Zaskoczeniem może być zaproponowany przez organ wyjątek w stosunku do obecnych klientów - jeżeli abonent lub użytkownik końcowy jest klientem dostawcy usług komunikacji elektronicznej, który uzyskał jego dane kontaktowe w związku ze sprzedażą produktów lub usług, dostawca ten może wykorzystywać te same środki (automatyczne systemy wywołujące, fakсы lub poczta elektroniczna) w celu marketingu bezpośredniego własnych podobnych produktów lub usług. W takiej sytuacji klient powinien mieć zapewnioną możliwość łatwego i bezpłatnego wniesienia sprzeciwu wobec takiego wykorzystania jego danych kontaktowych w momencie ich zbierania oraz przy każdej przesyłanej wiadomości.

Podstawy prawne przetwarzania danych

Przetwarzanie danych osobowych do celów marketingu bezpośredniego musi opierać się na jednej z podstaw prawnych wymienionych w art. 6 RODO. W praktyce najczęściej stosowane są **zgoda** (art. 6 ust. 1 lit. a RODO) oraz **uzasadniony interes administratora** (art. 6 ust. 1 lit. f RODO).

W przypadku zgody należy spełnić szereg wymagań – musi ona być dobrowolna, konkretna, świadoma i jednoznaczna, wyrażona w formie oświadczenia lub wyraźnego działania pozytywnego (np. zaznaczenie okienka, a nie jego odznaczenie).

Podstawowe zasady, o których należy pamiętać, stosując zgodę jako podstawę prawną przetwarzania danych:

- wykonanie umowy nie może być uzależnione od zgody na przetwarzanie danych do celów marketingowych, które nie są niezbędne do wykonania tej umowy;
- osoba, której dane dotyczą, musi mieć możliwość odmowy lub wycofania zgody bez poniesienia szkody;
- należy uzyskać odrębną zgodę na różne cele przetwarzania danych, nie należy stosować ogólnych przycisków typu "akceptuj wszystko";
- w kontekście cyfrowym wybór zgody powinien być jasny i podobny do innych dostępnych opcji;
- administrator musi być w stanie wykazać, że zgoda została udzielona – dowód zgody powinien być przechowywany nie dłużej niż jest to konieczne do spełnienia obowiązku prawnego lub obrony roszczeń;
- w przypadku przetwarzania danych wrażliwych zgoda musi być wyraźna;
- w przypadku małoletnich zgoda musi być świadoma, a informacje przekazywane w sposób dostosowany do ich wieku;

- wycofanie zgody musi być łatwe i bezpłatne; po wycofaniu zgody przetwarzanie danych musi zostać zakończone, chyba że istnieje inna podstawa prawna do ich dalszego przechowywania.

Uzasadniony interes administratora może stanowić podstawę prawną przetwarzania danych do celów marketingu bezpośredniego (motyw 47 RODO), jeżeli:

✓ administrator przeprowadzi test trzech kroków: identyfikacja uzasadnionego interesu, ocena niezbędności przetwarzania do realizacji tego interesu oraz test równowagi między interesami administratora a prawami i wolnościami osób, których dane dotyczą i uzyska pozytywny wynik,

✓ osoba, której dane dotyczą może mieć uzasadnione oczekiwania osób, których dane dotyczą, oparte na ich relacji z administratorem; osoba, która nigdy nie miała kontaktu z administratorem, zasadniczo nie będzie oczekiwać marketingu bezpośredniego.

W przypadku potencjalnych klientów, uzasadniony interes administratora jako podstawa prawna wymaga szczególnej ostrożności, ponieważ zazwyczaj osoby te nie mają oni jeszcze relacji z administratorem tj. punkt drugi powyżej może nie zostać spełniony.

Inne podstawy prawne, takie jak wykonanie umowy lub zadanie realizowane w interesie publicznym, generalnie nie są odpowiednie w kontekście marketingu bezpośredniego i raczej nie spotyka się użycia takich podstaw w praktyce.

Dlaczego prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO) nie do końca jest dobrą podstawą przetwarzania danych

W obliczu nowych regulacji prawnych oraz ich interpretacji coraz częściej podnosi się, że prawnie uzasadniony interes administratora może nie być odpowiednią podstawą do przetwarzania danych osobowych w marketingu bezpośrednim (oczywiście w pewnych okolicznościach). Chociaż motyw 47 RODO ogólnie wskazuje, że przetwarzanie danych osobowych do celów marketingu bezpośredniego można uznać za realizowane w prawnie uzasadnionym interesie, źródło wyraźnie zaznacza, że nie oznacza to automatycznie, iż będzie to ważna podstawa prawna.

Istnieją sytuacje, w których prawo wymaga zgody jako podstawy prawnej, co wyklucza możliwość polegania jedynie na uzasadnionym interesie. Najważniejszym przykładem jest sytuacja omawiana w niniejszym artykule tj. gdy marketing bezpośredni przybiera formę komunikacji elektronicznej (np. e-mail, SMS). W takim przypadku dyrektywa o prywatności i łączności elektronicznej (ePrivacy Directive) oraz jej transpozycja do prawa belgijskiego czy polskiego zasadniczo wymaga zgody osoby, której dane dotyczą na konkretny kanał komunikacji.

Ponadto, gdy przetwarzanie obejmuje dane wrażliwe w rozumieniu art. 9 ust. 1 RODO, wymagana jest wyraźna zgoda osoby, której dane dotyczą (art. 9 ust. 2 lit. a) RODO), co również wyklucza powołanie się na uzasadniony interes.

Nawet jeśli przepisy prawa nie wymagają zgody, powołanie się na uzasadniony interes jako podstawę prawną marketingu bezpośredniego wymaga spełnienia trzech warunków:

- test celu: marketing bezpośredni co do zasady może stanowić taki interes tj. cel promocji usług, produktów, marki administratora. Istnieją jednak wyjątki, np. promocja e-papierosów, która może być sprzeczna z innymi przepisami prawa;

- test konieczności: administrator musi wykazać, że nie można osiągnąć tego samego celu w inny sposób, bez przetwarzania danych osobowych lub przy mniejszej ingerencji w prywatność osób, których dane dotyczą;
- test równowagi (ważenia): interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, nie są nadrzędne wobec uzasadnionego interesu administratora.

W kontekście testu równowagi, uzasadnione oczekiwania osób, których dane dotyczą, oparte na ich relacjach z administratorem, odgrywają kluczową rolę. W przypadku potencjalnych klientów, którzy nie mają (jeszcze) relacji z administratorem, co do zasady nie mogą oni racjonalnie oczekiwać otrzymywania bezpośredniej komunikacji marketingowej. W takich sytuacjach, powołanie się na uzasadniony interes może być problematyczne i może nie przejść testu równowagi. Belgijski organ nadzoru podaje przykład sytuacji: gdy osoba kontaktuje się z wykonawcą w sprawie wyceny, ale ostatecznie korzysta z usług innego, to w zależności od okoliczności, pierwszy wykonawca może mieć uzasadniony interes, ale musi wykazać, że ten interes przeważa nad prawami osoby.

Podsumowując, prawnie uzasadniony interes administratora **nie zawsze jest odpowiednią podstawą do przetwarzania danych osobowych w marketingu bezpośrednim**, szczególnie w przypadku **komunikacji elektronicznej (gdzie zasadniczo wymagana jest zgoda)**, przetwarzania danych wrażliwych (gdzie wymagana jest wyraźna zgoda) oraz w sytuacjach, gdy **osoby, których dane dotyczą, nie mają uzasadnionych oczekiwań** co do otrzymywania takich komunikatów, a ich prawa i wolności mogłyby zostać naruszone. W każdym przypadku, administrator musi przeprowadzić **dokładną analizę i ocenę**, aby upewnić się, że wszystkie warunki powołania się na uzasadniony interes są spełnione, w tym przejść test celu, konieczności i równowagi.



O czym pamiętać przetwarzając dane osobowe w marketingu bezpośrednim

Przetwarzanie danych osobowych w procesie marketingu bezpośredniego będzie zgodne z prawem po spełnieniu następujących zasad:

- określenie celów przetwarzania jest kluczowe, opisanie celu jedynie jako "marketing bezpośredni" zazwyczaj nie jest wystarczające – taki ogólny opis nie umożliwia oceny jakości danych ani ustalenia, czy są one przetwarzane w sposób proporcjonalny;
- przestrzeganie zasady proporcjonalności (art. 5 ust. 1 lit. c) RODO), co oznacza, że dane osobowe muszą być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów przetwarzania;
- przestrzeganie zasady minimalizacji danych;
- określenie okresu przechowywania danych osobowych dla każdego celu przetwarzania (art. 5 ust. 1 lit. e) RODO), okres ten powinien być nie dłuższy niż jest to niezbędne do celów, dla których dane są przetwarzane, uwzględniając charakter relacji z osobą, której dane dotyczą oraz cykl życia promowanych produktów/usług. Dane potencjalnych klientów powinny być przechowywane krócej niż dane klientów. Po wycofaniu zgody lub wniesieniu sprzeciwu, dane

nie mogą być przechowywane do przyszłych celów marketingowych, których dotyczyło to działanie.

Zgoda czy zapłata

Interesującą kwestią którą porusza belgijski organ nadzoru w opublikowanych wytycznych jest temat „zgoda a zapłata”. Pojawia się on w kontekście dyskusji o dobrowolności zgody na przetwarzanie danych osobowych, w odniesieniu m.in. do reklamy behawioralnej na głównych platformach internetowych.

Zalecenie odnosi się do wyroku Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z lipca 2023 r., który dotyczył ważności zgody uzyskanej przez Meta (Facebook) w odniesieniu do wyświetlania reklam. W tej sprawie TSUE rozważał sytuację, w której użytkownicy musieli wybrać między wyrażeniem zgody na przetwarzanie ich danych do celów reklamy behawioralnej a zapłaceniem za brak takiego przetwarzania.

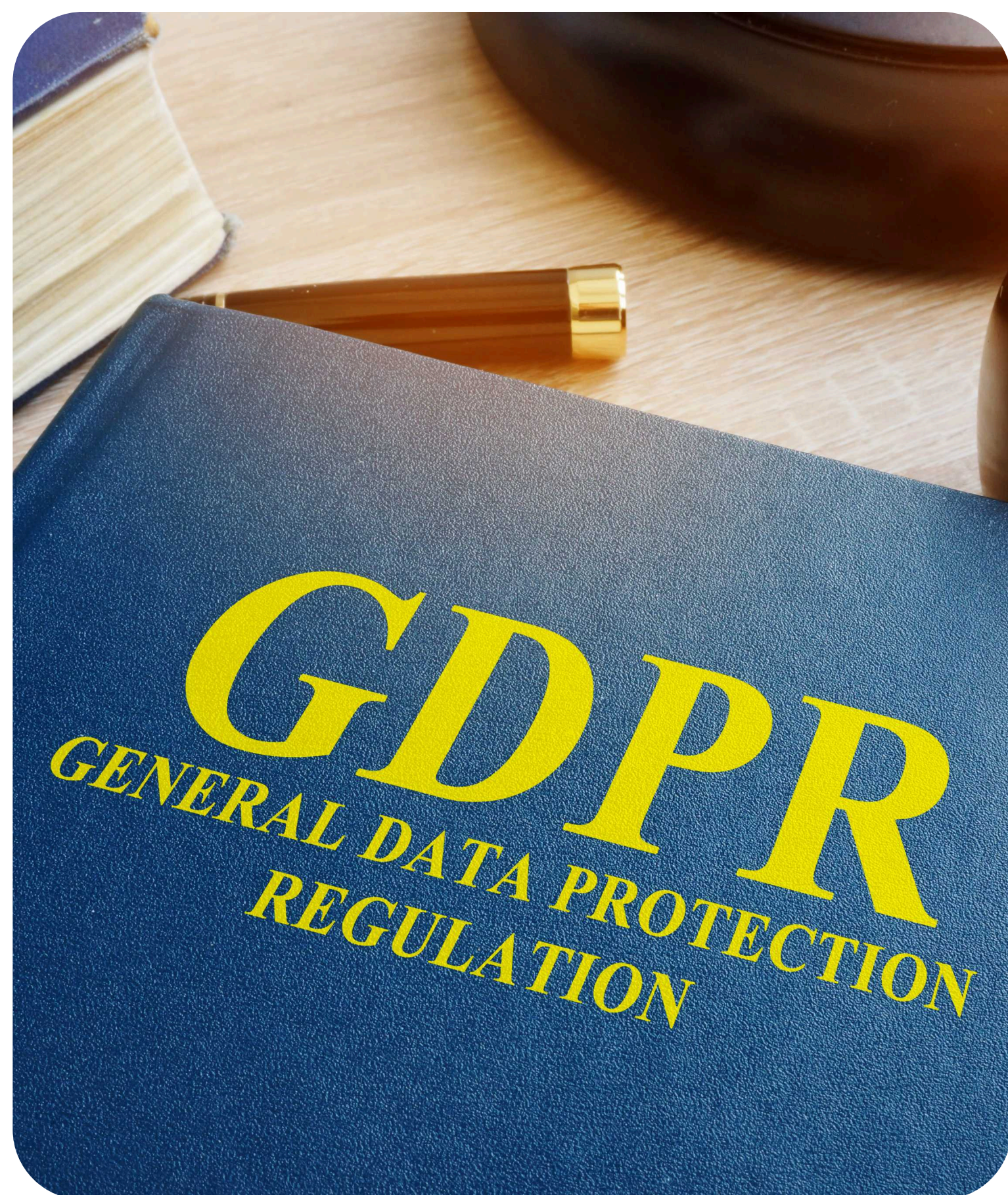
W kontekście dobrowolności zgody, TSUE zauważył, że utrata korzyści lub usługi w przypadku odmowy wyrażenia zgody może pozbawić możliwości rzeczywistej swobody wyboru i stanowić szkodę w rozumieniu motywu 42 RODO, co oznacza, że zgoda nie jest uznawana za wyrażoną dobrowolnie. TSUE, a w ślad za nim belgijski UODO sugeruje, że wymóg dobrowolności może zostać spełniony, jeżeli operator zaoferuje alternatywę.

Zalecenie przywołuje ponadto opinię Europejskiej Rady Ochrony Danych (EROD) z kwietnia 2024 r. w sprawie ważności zgody w kontekście modeli "zgoda lub zapłata" stosowanych przez duże platformy internetowe, które opierają się na zgodzie jako podstawie prawnej przetwarzania danych osobowych do celów reklamy behawioralnej. EROD uważa, że co do zasady zgoda nie będzie

uznawana za ważną, gdy użytkownicy stają przed jedyną binarną opcją "zgoda lub zapłata". Aby móc wykazać, że uzyskały ważną zgodę, platformy powinny oferować bezpłatną alternatywę dla opcji binarnej.

W każdym przypadku, jeśli wymagana jest płatność za uniknięcie przetwarzania danych do celów reklamy behawioralnej, taka płatność nie może skutkować tym, że w praktyce uniemożliwia użytkownikom dokonanie swobodnego wyboru (na przykład, jeśli kwota jest zbyt wysoka).

Modele "zgoda lub zapłata" budzą wątpliwości co do dobrowolności zgody w kontekście reklamy behawioralnej. Zarówno TSUE, jak i EROD podkreślają, że użytkownicy powinni mieć możliwość dokonania rzeczywistego i swobodnego wyboru, co może oznaczać konieczność zaoferowania bezpłatnej alternatywy dla tych, którzy nie chcą wyrazić zgody na przetwarzanie danych w zamian za dostęp do usług. Opłata za brak przetwarzania nie może być również na tyle wysoka, by de facto uniemożliwić swobodny wybór.



Czy wytyczne belgijskiego UODO są zgodne z aktualnym stanowiskiem polskich organów nadzoru?

W 2024 roku UOKiK, UODO i UKE zaostrzyły podejście do marketingu bezpośredniego, koncentrując się na ochronie konsumentów, zgodności z RODO oraz wymogu uzyskania wyraźnej zgody na kontakt marketingowy. Oto najważniejsze aktualne wytyczne:

Urząd Ochrony Konkurencji i Konsumentów (UOKiK) skupił się na walce z agresywnym telemarketingiem (szczególnie w branży fotowoltaicznej i ubezpieczeniowej), wydając szereg decyzji zwrócił uwagę na:

- zakaz domniemywania zgody – zgoda na marketing musi być wyrażona wprost, nie można jej domniemywać z np. braku sprzeciwu czy bierności osoby;
- przejrzystość przekazu – konsumenci muszą od początku rozmowy wiedzieć, kto dzwoni, w jakim celu i skąd ma ich dane;
- zakaz wprowadzania w błąd – nie można sugerować, że klient musi zawrzeć umowę lub że dzwoni się „w imieniu operatora” (np. Orange, PGE), jeśli tak nie jest.
- proste wycofanie zgody – klient musi mieć możliwość szybkiego i skutecznego wycofania zgody na kontakt.

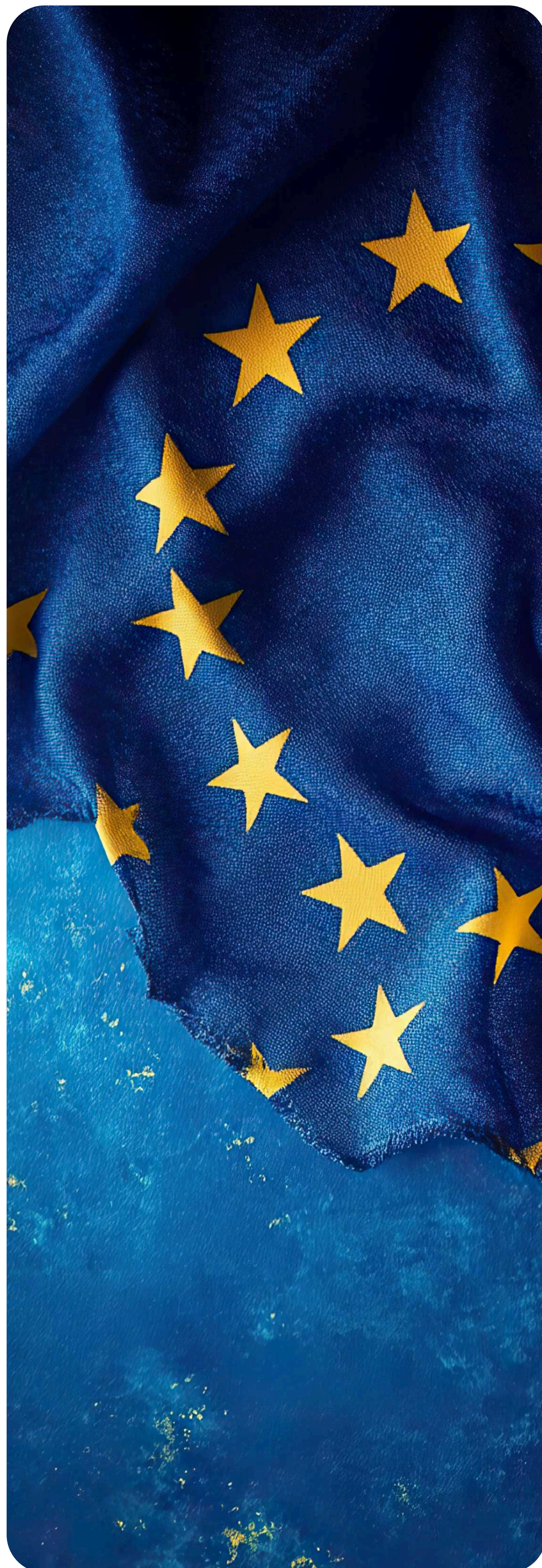
Urząd Ochrony Danych Osobowych (UODO) w 2024 r. zintensyfikował kontrole w zakresie przetwarzania danych w celach marketingowych wskazując jednocześnie, że:

- zgoda musi być dobrowolna i konkretna – nie może być ukryta w regulaminie ani wymuszona przy zakupie;

- zakaz domniemywania zgody – zgoda na marketing musi być wyrażona wprost, nie można jej domniemywać z np. braku sprzeciwu czy bierności osoby;
- prawo do sprzeciwu – jeśli klient sprzeciwi się przetwarzaniu jego danych w celach marketingowych, firma musi natychmiast zaprzestać działań;
- obowiązek informacyjny – każda osoba musi wiedzieć, kto jest administratorem jej danych i jak może się sprzeciwić dalszemu kontaktowi;
- nielegalne kupowanie baz danych – firmy nie mogą korzystać z baz danych pochodzących z niepewnych źródeł (np. zakupionych bez zgody osób, których dane dotyczą).

Urząd Komunikacji Elektronicznej (UKE) stanął przed wyzwaniem monitorowania zgodności prowadzonych działań marketingowych w odniesieniu do nowej ustawy Prawo Komunikacji Elektronicznej (PKE). Najważniejsze zmiany i wytyczne UKE to:

- obowiązek uzyskania zgody na telemarketing – każda rozmowa telefoniczna z ofertą wymaga wcześniejszej, wyraźnej zgody klienta;
- zakaz automatycznych systemów dzwoniących bez zgody – boty dzwoniące w celach marketingowych bez uprzedniej zgody są nielegalne;
- nowe sankcje – kary za nielegalny marketing mogą wynieść do 3% rocznych przychodów firmy.



Kluczowe zmiany i wytyczne

- ✔ informowanie klientów o nowych produktach i usługach
- ✔ inicjowanie sprzedaży produktów i/lub usług
- ✔ profilowanie klientów

Jeśli Twoja firma prowadzi marketing bezpośredni, warto przeanalizować procedury i upewnić się, że spełniasz najnowsze wymogi

Podsumowanie

Podsumowując, prawnie uzasadniony interes administratora **nie jest zawsze odpowiednią podstawą do przetwarzania danych osobowych w marketingu bezpośrednim**, szczególnie w przypadku **komunikacji elektronicznej (gdzie zasadniczo wymagana jest zgoda)**, przetwarzania danych wrażliwych (gdzie wymagana jest wyraźna zgoda) oraz w sytuacjach, gdy **osoby, których dane dotyczą, nie mają uzasadnionych oczekiwań** co do otrzymywania takich komunikatów, a ich prawa i wolności mogłyby zostać naruszone. W każdym przypadku, administrator musi przeprowadzić **dokładną analizę i ocenę**, aby upewnić się, że wszystkie warunki powołania się na uzasadniony interes są spełnione, w tym przejść test celu, konieczności i równowagi.

Kary za nielegalne połączenia marketingowe

UKE



Orange -9,1 mln zł kary (2023)

Za co? Nielegalne połączenia marketingowe do klientów bez wcześniejszej zgody.



Virgin Mobile - 1,9 mln zł kary (2022)

Za co? Automatyczne systemy telemarketingowe dzwoniły do klientów bez ich zgody.

UODO



ClickQuick Sp. z o.o – 201 tys., zł (2020)

Za co? wykonywanie połączeń marketingowych bez zgody odbiorców i brak zapewnienia możliwości realizacji przysługujących praw (np. prawa do sprzeciwu wobec przetwarzania danych).

Login Account

☐ Remember me[Forgot Password?](#)

Maciej Kołodziej

Data Protection & Information Security Expert

AAA+, czyli jak zidentyfikować, dopuścić do korzystania z zasobów i rozliczyć działalność użytkownika w systemach przetwarzania informacji

Tematyka zarządzania tożsamością oraz uprawnieniami w systemach teleinformatycznych stanowi istotne wyzwanie dla dysponentów zasobów informacyjnych. Mimo odmiennych wymagań szczegółowych (stawianych przez regulacje dotyczące bezpieczeństwa informacji, ochrony danych osobowych czy przepisy branżowe), osoba odpowiedzialna za proces identyfikacji oraz dopuszczania do zasobów użytkowników, systemów i urządzeń, mających dostęp do danych, powinna za każdym razem podjąć starania mające na celu zaplanowanie zasad, przeprowadzenie analizy ryzyk i sformalizowanie procesu korzystania z zasobów.

Administratorzy IT mają często wątpliwości, jakie zastosować środki i jak właściwie zorganizować ochronę danych przetwarzanych na stacjach roboczych, urządzeniach mobilnych w serwerach, repozytoriach i serwisach. **Źle zabezpieczone komputery, laptopy, tablety, smartfony, pendrive'y i dyski przenośne – to najsłabsze (zaraz po człowieku) ogniwa infrastruktury IT.** Projektując systemy przetwarzania informacji należy jednak uwzględnić także zagrożenia dotyczące systemów informatycznych, ich konfiguracji, ochrony, zarządzania i eksploatacji.

Identyfikacja użytkowników systemów, przydzielanie im uprawnień oraz nadzór i rozliczalność ich aktywności jest jednym z kluczowych elementów ochrony. Przepisy oraz dobre praktyki wskazują na konieczność dopuszczania do przetwarzania informacji jedynie uprawnionych użytkowników, z uwzględnieniem podziału na kategorie: osoby/operatorzy, aplikacje/systemy i urządzenia.

Projekty bezpieczeństwa najczęściej bazują na trzyprocesowym modelu AAA+ opisującym zasady:

Uwierzytelnienie (ang. Authentication), czyli weryfikacja tożsamości użytkownika zamierzającego uzyskać dostęp do zasobu;

Autoryzacja (ang. Authorisation), czyli ustalenie uprawnień w systemie dla zidentyfikowanego użytkownika;

Rozliczalność (ang. Accounting), zapewniająca rejestrację wszystkich operacji użytkownika związanych z dostępem i wykorzystywaniem zasobów systemu.

często uwzględnia się również czwartą zasadę:

Audytowalność (ang. Auditing), pozwalającą na dodatkowe, niezależne kontrolowanie

🔗 poprawności całego procesu i jakości informacji zarejestrowanych w ramach rozliczalności w systemie.

Uwierzytelnienie użytkownika

Pierwszym etapem w procesie identyfikacji jest ustalenie, czy osoba, aplikacja, system lub urządzenie, które zgłaszają zapotrzebowanie na dostęp do zasobów są tym, za kogo się podają. Dość duża łatwość podszycia się pod tożsamość w świecie cyfrowym wymaga stosowania skutecznych, powtarzalnych i odpowiednio chronionych mechanizmów pozwalających zweryfikować, kto chce skorzystać z zasobów.

Weryfikacja tożsamości w procesie uwierzytelnienia odbywa się najczęściej poprzez podanie unikalnego identyfikatora użytkownika, którym może być adres e-mail służący do utrzymania kontaktu technicznego, oraz wykorzystania drugiego składnika identyfikującego, wybieranego w oparciu o jeden z czterech rodzajów kryteriów:



Kryterium wiedzy: „coś, co wiesz”

gdy stosowane są hasła, kody PIN, wzory graficzne lub inne poufne informacje, którymi dysponuje użytkownik;



Kryterium posiadania: „coś, co masz”

jeśli dla skutecznego potwierdzenia tożsamości zachodzi konieczność skorzystania z dodatkowego wsparcia technicznego, np. poprzez skorzystanie z kluczy sprzętowych, tokenów, kart magnetycznych/chipowych lub innych urządzeń podpinanych do terminala końcowego lub wykorzystywanych w procesie weryfikacji (np. przepisanie udostępnianych w tokenie kodów, wysłanie równoległe komunikatów przez sieć komputerową, wykorzystanie mechanizmów wieloskładnikowego uwierzytelnienia xFA);



Kryterium kontroli cech osobowych: „to, kim jesteś”

gdy podczas weryfikacji wykorzystywane są zabezpieczenia typu CAPTCHA, wymagające aktywnego, „rozumnego” działania ze strony użytkownika i rozwiązywania np. zagadek logicznych albo gdy do identyfikacji zastosowano metody biometryczne lub pseudobiometryczne, odwzorowujące cechy osobowe w bardziej prymitywny, ale wystarczająco skuteczny i powtarzalny sposób, np. porównując podobieństwo obrazów linii papilarnych albo przetworzone zdjęcia użytkowników w miejsce pełnej analizy biometrycznej;

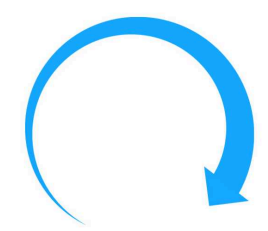


Kryterium zaufania do strony trzeciej: „wiedza i zewnętrzne decyzje”

jeśli decyzje o pozytywnej weryfikacji podejmowane są w oparciu o informacje pozyskiwane z innych systemów uwierzytelniających, względem których zbudowano relację zaufania, wynikającą z oceny własnej, opinii branżowej lub wskazań w procesie (np. odwołania do systemów partnerów lub wskazanych przez klientów, dla których świadczone są usługi). Wynik weryfikacji zależy od decyzji podmiotów trzecich udostępniających inne, zewnętrzne systemy uwierzytelniające lub np. rozwiązania klasy SSO (Single Sign On), z których korzystają użytkownicy i oczekują transparentnej współpracy z systemem usługodawcy. Do tej kategorii można też zaliczyć konieczność potwierdzania tożsamości przez drugą osobę (tzw. metoda dwóch kluczy lub drugich oczu);



I'm not a robot



CAPTCHA

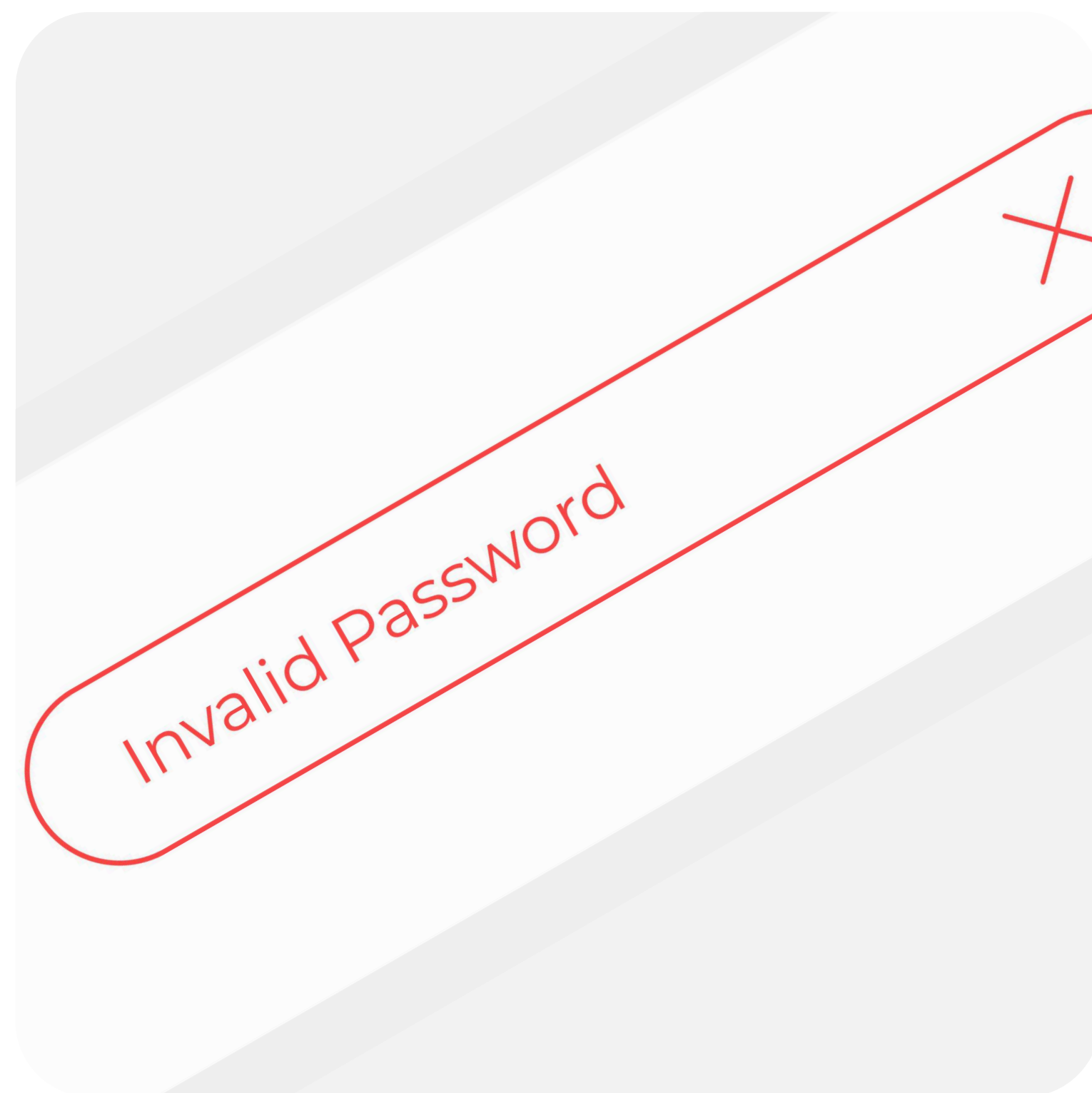
Uwierzytelnienie użytkownika

Hasła, kody PIN, wzory graficzne lub inne poufne informacje, którymi dysponuje użytkownik

Statystycznie, do potwierdzenia swojej tożsamości podczas logowania do systemów, użytkownicy najczęściej wykorzystują hasła. Temat haseł został szczegółowo opisany w newsletterze RODO LexDigital nr 12/2024. W artykule przedstawiliśmy szczegółową analizę zasad stosowania, wskazaliśmy na wymogi formalno-prawne oraz omówiliśmy najważniejsze zalecenia z zakresu bezpieczeństwa stosowania haseł. Aby chronić swoją cyfrową tożsamość i zabezpieczyć się przed ewentualnym przejęciem kontroli nad zasobami, do których został im przyznany dostęp użytkownicy powinni zadbać o to, aby hasła były chronione przed ich kompromitacją (czyli ujawnieniem, wykradzeniem lub zapoznaniem się przez osobę nieupoważnioną) i nie były zbyt proste – rekomenduje się opracowanie zaleceń dotyczących odpowiedniej długości, złożoności i unikalności haseł.

Zaleca się stosowanie mnemotechnicznych zasad zapamiętywania haseł lub używanie specjalnych programów, tzw. managerów haseł, które pozwalają stosować hasła lepszej jakości (dłuższe, niesłownikowe, unikalne) oraz zapewniają lepszą ich ochronę.

Jeśli użytkownik zapomni hasła lub np. na podstawie analizy zachowania użytkownika system będzie wymagał podania dodatkowych informacji można zastosować (zdefiniowane wcześniej w profilu) pytania pomocnicze, a od poprawnej odpowiedzi uzależnić wynik procesu uwierzytelnienia.



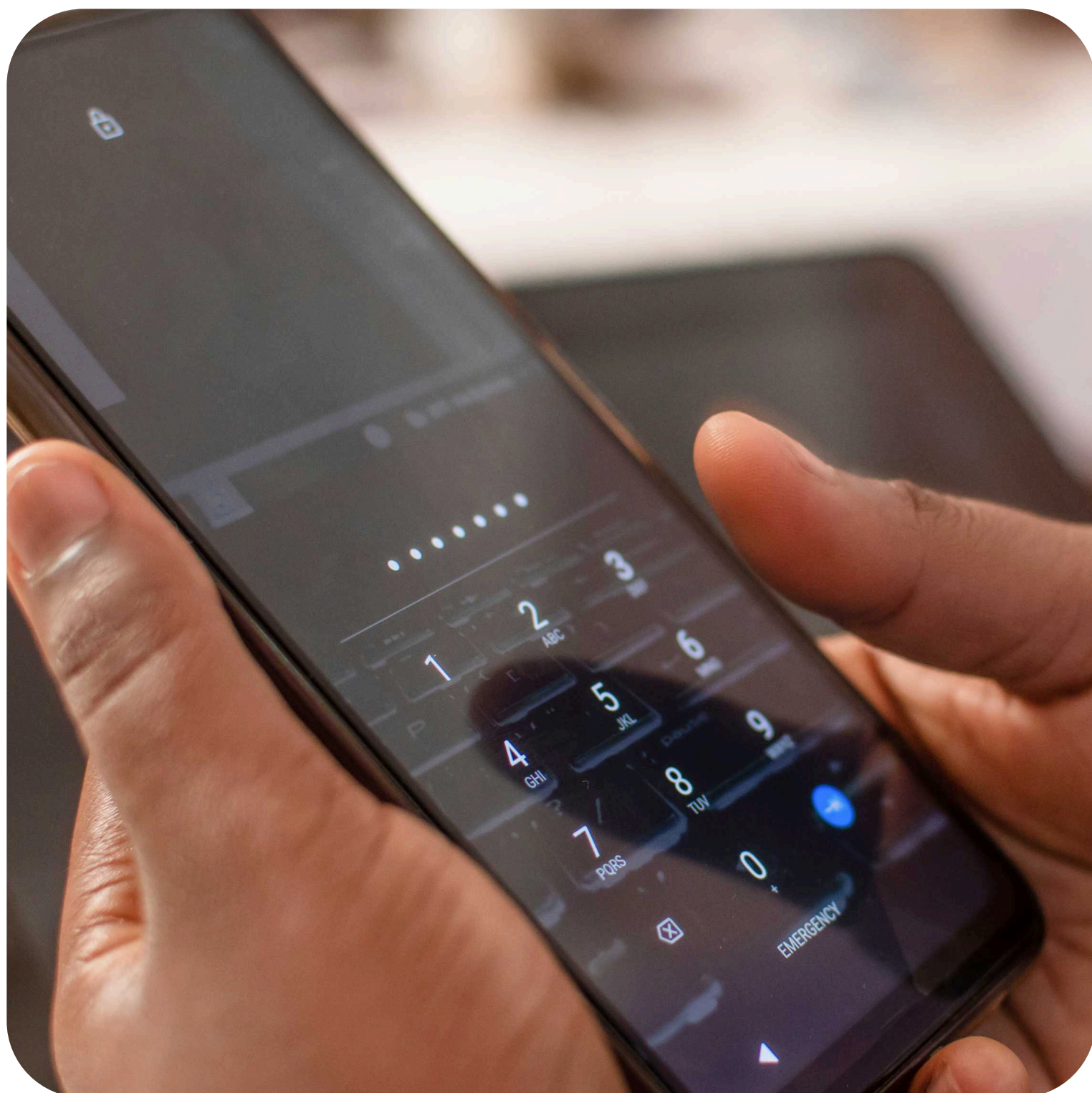
W przypadku, gdy komunikacja jest nawiązywana przez inne systemy lub urządzenia za ochronę atrybutów je identyfikujących (w tym identyfikatorów, haseł i konfiguracji) odpowiadają ich administratorzy.



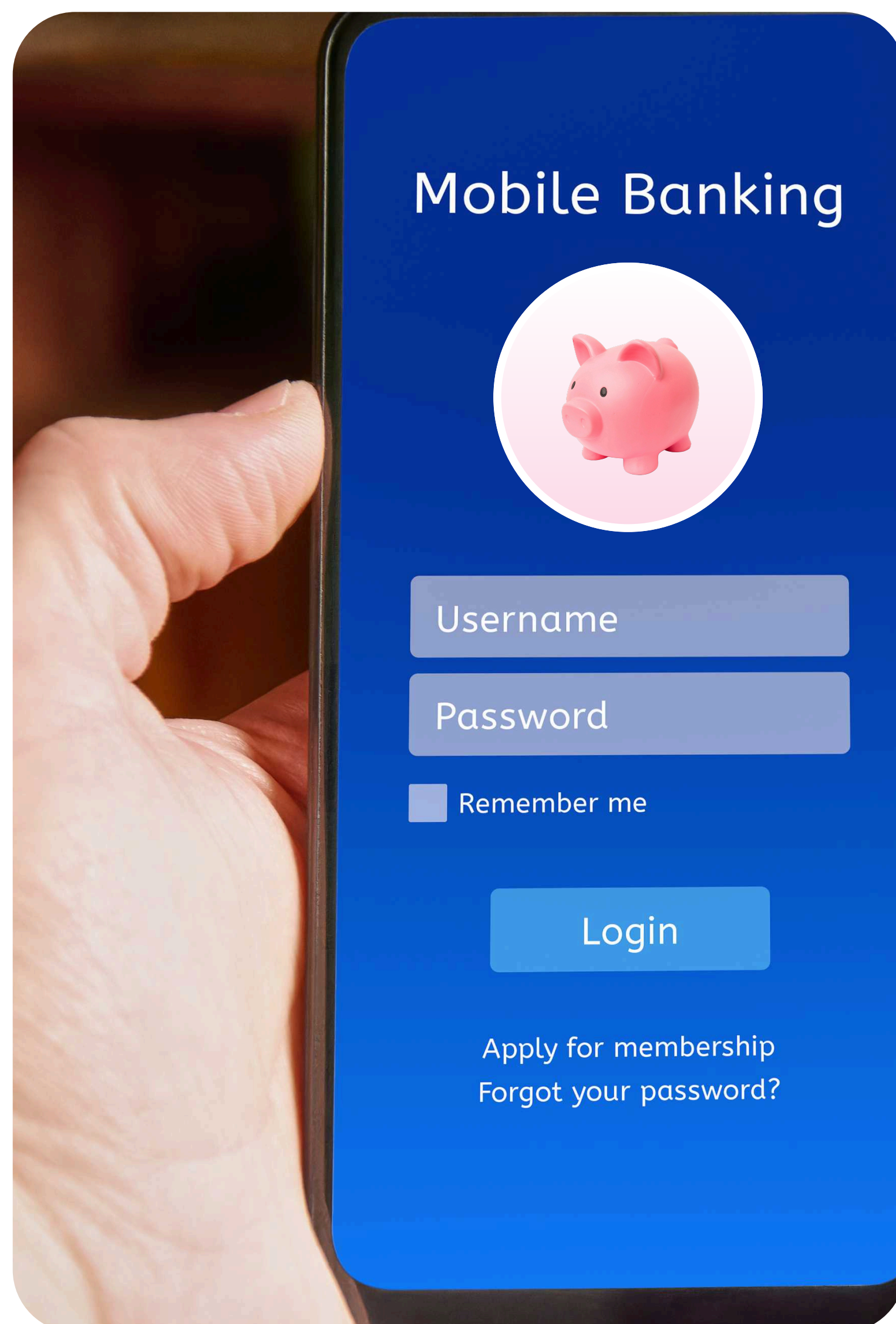
Pozostałe metody uwierzytelniania (inne niż hasłem), stają się coraz bardziej popularne i są stosowane jako uzupełnienie procesu lub równolegle z hasłami, aby ułatwić korzystanie z systemów oraz zoptymalizować procesy nadzoru nad użytkownikami i udostępnianymi im zasobami.

Dobłą praktyką jest dodatkowe stosowanie haseł lub kodów PIN, nie tylko jako atrybutów logowania, ale też do wstępnego ograniczenia możliwości korzystania z urządzeń, z pomocą których użytkownik uzyskuje dostęp do danych. Przykładem może być logowanie do urządzenia z wykorzystaniem krótkiego, lokalnie zdefiniowanego kodu PIN, który w rzeczywistości jest uproszczonym drugim etapem uwierzytelnienia, po wcześniejszym przeprowadzeniu

pełnej procedury identyfikacyjnej z użyciem hasła lub innego silniejszego mechanizmu i odnotowaniem lokalnie, na urządzeniu, niezbędnych atrybutów bezpieczeństwa, np. tokenów lub informacji uwierzytelniających, które będą chronione i dostępne lokalnie oraz przekazywane w przypadku koniecznej transmisji do zaufanych systemów zewnętrznych.



Warto wskazać też na funkcjonalność, która nie jest wprawdzie popularna, ale daje możliwość zwiększenia bezpieczeństwa procesu uwierzytelnienia i logowania do systemów i usług. Taką funkcjonalnością jest dwustronne uwierzytelnienie, w którym nie tylko użytkownik podaje do systemu informacje o sobie, ale ma też możliwość zweryfikować czy system z którym się połączył jest tym systemem, za który się on podaje. W tym celu ekran logowania zawiera dodatkowe informacje wyświetlane w kontekście logującego się użytkownika, gdy ten wstępnie się przedstawi (np. poda login). Na zdjęciu widać, że system wyświetla zdefiniowany w profilu użytkownika obrazek (może to być też np. dodatkowy napis, specyficzny układ okna logowania itp.), na którego podstawie użytkownik może zweryfikować, zanim poda hasło, czy może zaufa, że połączył się z właściwą stroną logowania. Oczywiście każde zabezpieczenie może zostać złamane lub zmodyfikowane, ale stosowanie tego typu rozwiązań podnosi zaufanie, bezpieczeństwo, czujność i zmniejsza prawdopodobieństwo błędów.



Zapasowe hasła w kopercie

Mając na uwadze sytuacje nadzwyczajne, administratorzy systemów mogą przygotować nośniki zawierające „hasła ostatniej szansy”, czyli specjalnie tworzone i chronione kody, hasła lub inne instrumenty bezpieczeństwa pozwalające na dostęp do zasobów i ich zarządzania, które okazują się przydatne, gdy zawiedzie człowiek, jego pamięć lub dostępność, a konieczne jest kontynuowanie procesu. Na nośnikach tych (np. na szyfrowanych pendrive'ach lub w kopertach) może być przechowywane np. aktualne hasło do dodatkowego konta administracyjnego systemu, kanału komunikacji, bazy danych lub innej chronionej usługi lub zasobu. Należy przewidzieć procedurę umożliwiającą skorzystanie z tego nośnika w określonych sytuacjach oraz zasady zobowiązujące administratorów przygotowywania takich nośników i utrzymania ich aktualności.

Kryterium posiadania

Wsparcie techniczne, klucze, tokeny, karty, xFA

W zależności od decyzji dostawcy usługi uwierzytelnienia może ona być wspierana rozwiązaniami technicznymi, które muszą być dostępne dla użytkownika i wykorzystywane podczas procesu uwierzytelnienia lub nawet dłużej, przez cały czas korzystania z udostępnianych zasobów. Przykładowe rozwiązania zostały przedstawione poniżej. Są wśród nich starsze modele tokenów sprzętowych generatorów haseł jednorazowych zmiennych w funkcji czasu, dostarczane jako sprzęt lub oprogramowanie, wspierane dodatkowo przez klawiatury kodowe, a także czytniki kart chipowych, których posiadanie i wykonywane operacje potwierdzają tożsamość użytkownika. Warto również wspomnieć o kluczach bezpieczeństwa YubiKey, które są wpinane lub komunikujące się z urządzeniami po NFC, wspierające procesy 2FA.



Uwierzytelnianie wieloskładnikowe xFA (zwane również weryfikacją dwu- lub wielopoziomową) jest rozwiązaniem polegającym na stosowaniu podczas uwierzytelnienia dodatkowych mechanizmów zabezpieczających, które powinny działać w innym kanale komunikacyjnym. Stosując 2FA użytkownik musi przedstawić do systemu drugi atrybut weryfikujący tożsamość, np.:

- PIN otrzymany w wiadomości SMS wysłanej na numer telefonu w profilu osoby,
- Tekst odczytany z wiadomości e-mail wysłanej na podany w profilu adres e-mail,
- Informację wygenerowaną w aplikacji uwierzytelniającej,
- Kontrolę komunikacji przez wysłanie komunikatu (push) w aplikacjach,
- Kod odczytany ze sprzętowego tokenu, wkładając do specjalnego czytnika klucz cyfrowy (np. USB) lub kartę chipową,
- Identyfikację biometryczną (np. linii papilarnych, oka lub kształtu części ciała).
- Połączenie z urządzeniem identyfikującym (telefon przez NFC, Bluetooth, WiFi)
- Połączenie z konkretnego adresu IP (wskazany adres, grupa adresów, sieć, kraj),
- Certyfikat osoby, aplikacji lub urządzenia przekazywany w trakcie połączenia.

aby wyeliminować przekazanie informacji, które np. są zapisane w pamięci przeglądarki i mogły zostać przejęte lub przypadkowo podane. W takiej sytuacji drugi lub kolejny składnik uwierzytelnienia chroni przed pomyłkami lub nadużyciami. Podanie poprawnych informacji kończy proces, a podanie złych może uruchomić działania awaryjne.



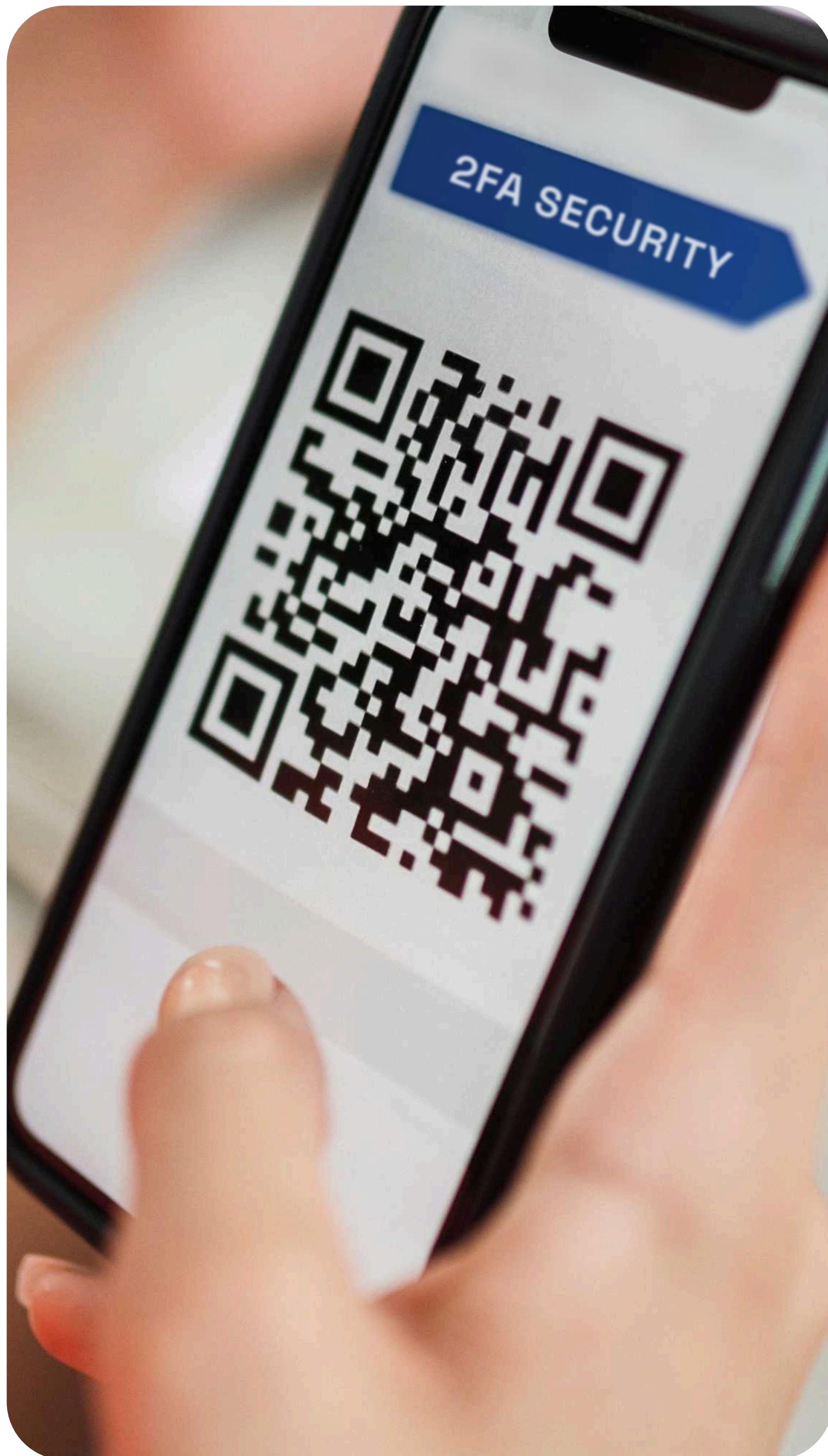
Należy zwrócić uwagę na poważny problem związany z xFA:

Często się zdarza, że wszystkie atrybuty użyte do uwierzytelnienia (np. login, hasło i kod SMS) udostępniane są z tego samego urządzenia, na które trafiają. Może to spowodować, że złośliwe oprogramowanie samo skorzysta z informacji, przechwyconych np. narzędziem do rejestracji danych z klawiatury, wygeneruje potrzebę

Kryterium kontroli cech osobowych

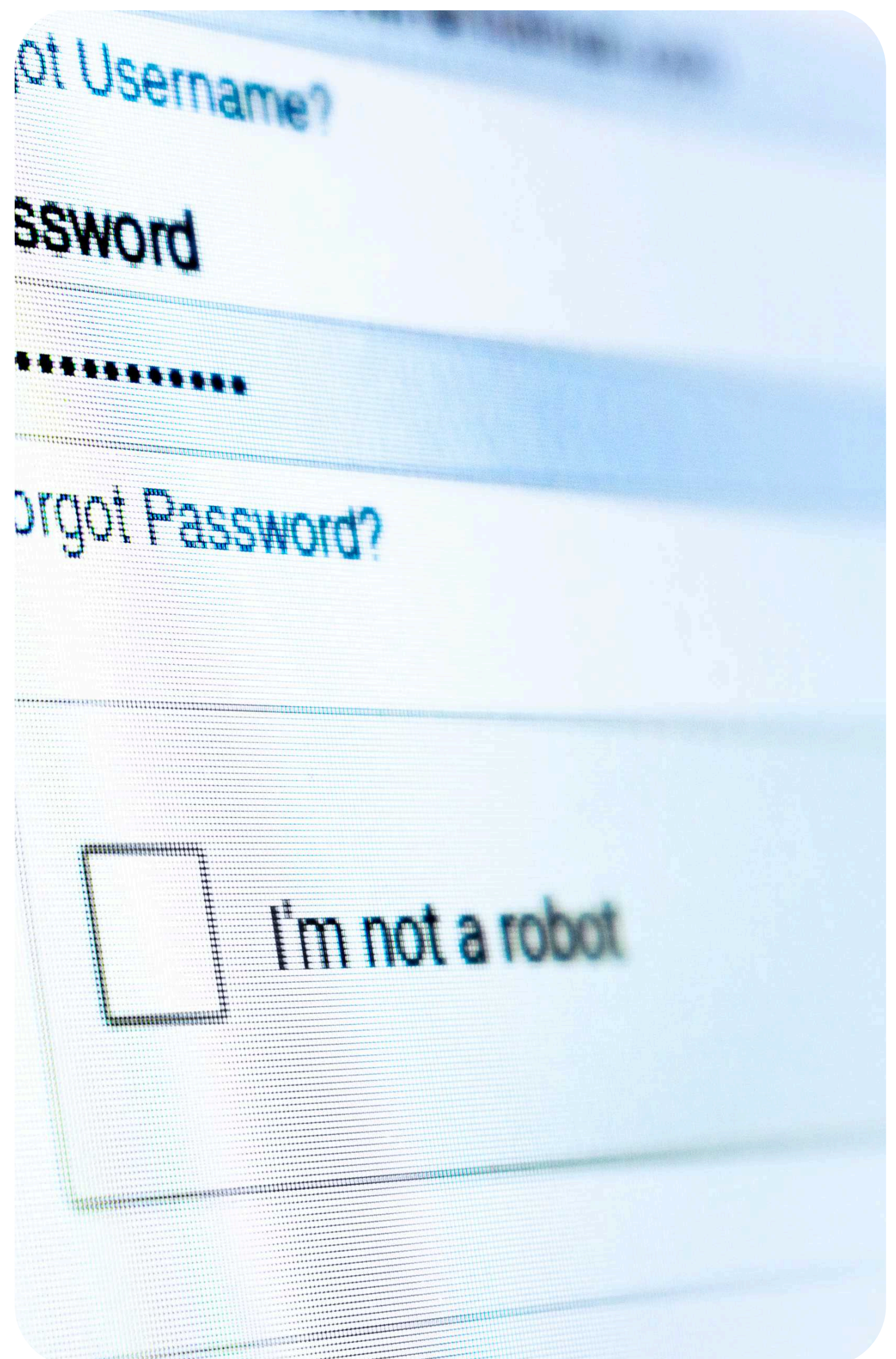
Zabezpieczenia typu CAPTCHA, biometria

Dość popularne zabezpieczenia typu CAPTCHA (ang. Completely Automated Public Turing test to tell Computers and Humans Apart), wspierające proces uwierzytelnienia, zmieniające z upływem czasu stopień skomplikowania i stawiane przed użytkownikiem wymogi, wymagające aktywnego, „rozumnego” działania ze strony użytkownika, mające na celu wyeliminowanie zautomatyzowanego przetwarzania i przełamania mechanizmów ochrony stają się coraz mniej efektywne, ze względu na wykorzystywanie systemów sztucznej inteligencji, które systematycznie i skutecznie potrafią rozwiązać zadania i ominąć to zabezpieczenie.



otrzymania dodatkowego kodu, odczyta go i wprowadzi do systemu bez udziału użytkownika, co skompromituje stosowane rozwiązanie.

Zalecane jest więc, aby rozdzielić kanały komunikacji dla xFA pomiędzy różne urządzenia. Przykładowo, jeśli proces uwierzytelnienia (logowania) ma miejsce z telefonu komórkowego, to informacje do 2FA powinny trafić na komputer np. pocztą elektroniczną (pod warunkiem że na smartfonie nie ma uruchomionego programu pocztowego) lub komunikatorem (pod warunkiem że będzie to kopia uruchomiona na komputerze, a wiadomość nie dotrze na kopię aplikacji uruchomioną na smartfonie). Jeśli natomiast logowanie ma miejsce z komputera, to na powiązany z użytkownikiem i wskazany w profilu numer telefonu można wysłać SMS-a z kodem, lub skierować na telefon komunikat metodą Push.



Inną interesującą funkcjonalnością jest identyfikacja użytkownika wspierana przez metody biometryczne, pozwalające w sposób wysoce prawdopodobny potwierdzić tożsamość użytkownika.

Niestety nie wszystkie dostępne rozwiązania korzystają z rzeczywistych analiz biometrycznych, ponieważ wymagają one dość złożonej analizy wielu składowych cech osoby i są wymagające obliczeniowo, przez co mogą niepotrzebnie obciążać terminal/urządzenie końcowe, z którego korzysta użytkownik.

Jako kompromis stosuje się funkcjonalności o cechach biometrycznych wykorzystujące rozwiązania prostsze, odwzorowując cechy osobowe w bardziej prymitywny, ale wystarczająco skuteczny, powtarzalny i wystarczający dla wymaganego poziomu bezpieczeństwa większości zastosowań sposób, np. porównując podobieństwo obrazów linii papilarnych albo przetworzone zdjęcia użytkownika w miejsce pełnej analizy biometrycznej.



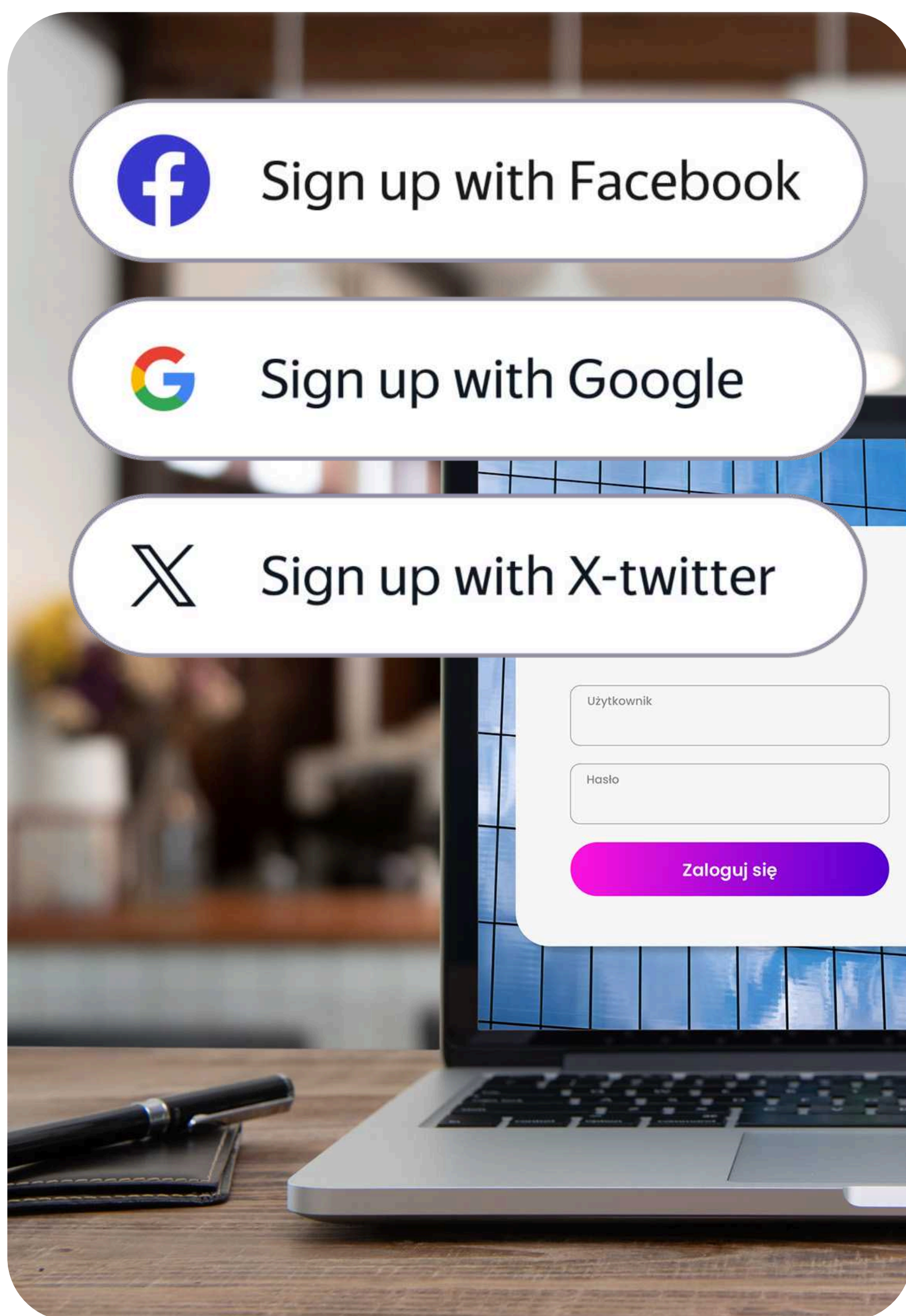
Kryterium zaufania do strony trzeciej

Decyzje z zaufanych systemów zewnętrznych, SSO, metoda dwóch kluczy lub drugich oczu

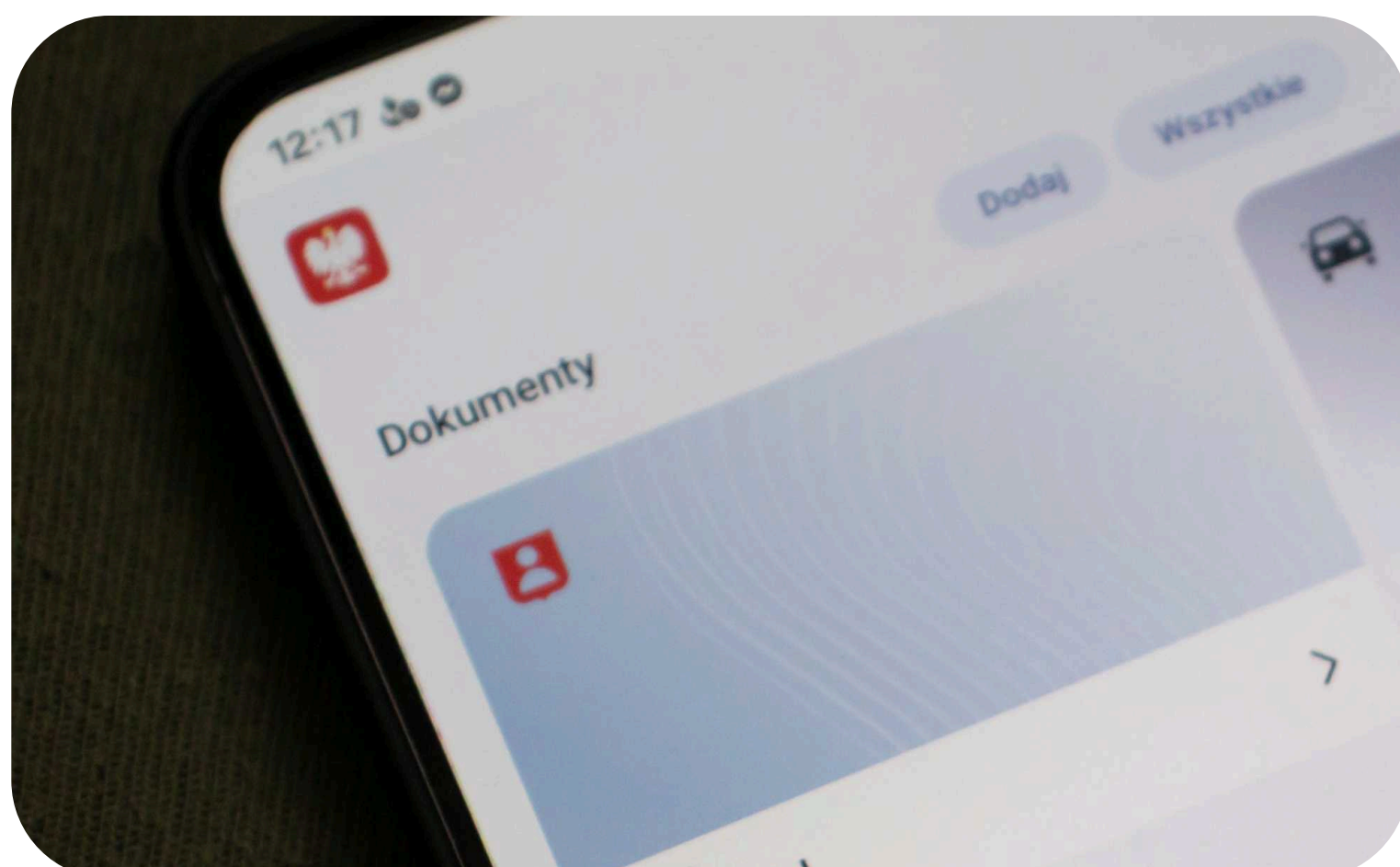
Coraz większą popularność zdobywają rozwiązania hybrydowe, które, oprócz własnych rozwiązań i lokalnych baz oraz mechanizmów pozwalających zidentyfikować użytkowników, korzystają z pomocy z strony zewnętrznych dostawców usług uwierzytelnienia. Wśród rozwiązań należy wskazać platformy (takie jak Microsoft Entra ID, wcześniej znane jako Azure Active Directory, albo OKTA) obsługujące wielu użytkowników, integrujące wiele systemów i zapewniające mechanizmy potwierdzania tożsamości, jeśli system dziedziny będzie w relacji zaufania.

Tego typu rozwiązania można zintegrować przeźroczyście dla użytkownika, który w pierwszej fazie musi uwierzytelnić się w odpowiednim systemie, aby potem odpowiednie informacje o nim były przekazywane transparentnie, na żądanie, do innych systemów, które będą świadczyły użytkownikowi usługi bez dodatkowego procesu weryfikacji jego tożsamości. Raz zweryfikowany użytkownik będzie mógł więc korzystać z wielu usług w różnych miejscach, bez konieczności dodatkowych procedur uwierzytelnienia, pod warunkiem że będzie istniała odpowiednia sieć powiązań, zależności i konfiguracji między punktami uwierzytelnienia będącymi w relacjach wzajemnego zaufania. Tego typu rozwiązania są również udostępniane przez popularne serwisy społecznościowe, które pod warunkiem zgody wyrażonej przez użytkownika, mogą przekazywać informacje i dotyczące go parametry do innych systemów i aplikacji.

Wiele krajów wspiera możliwość integracji systemów teleinformatycznych poprzez wdrażanie systemów uwierzytelnienia dla infrastruktury administracji i oficjalnych systemów informacyjnych.

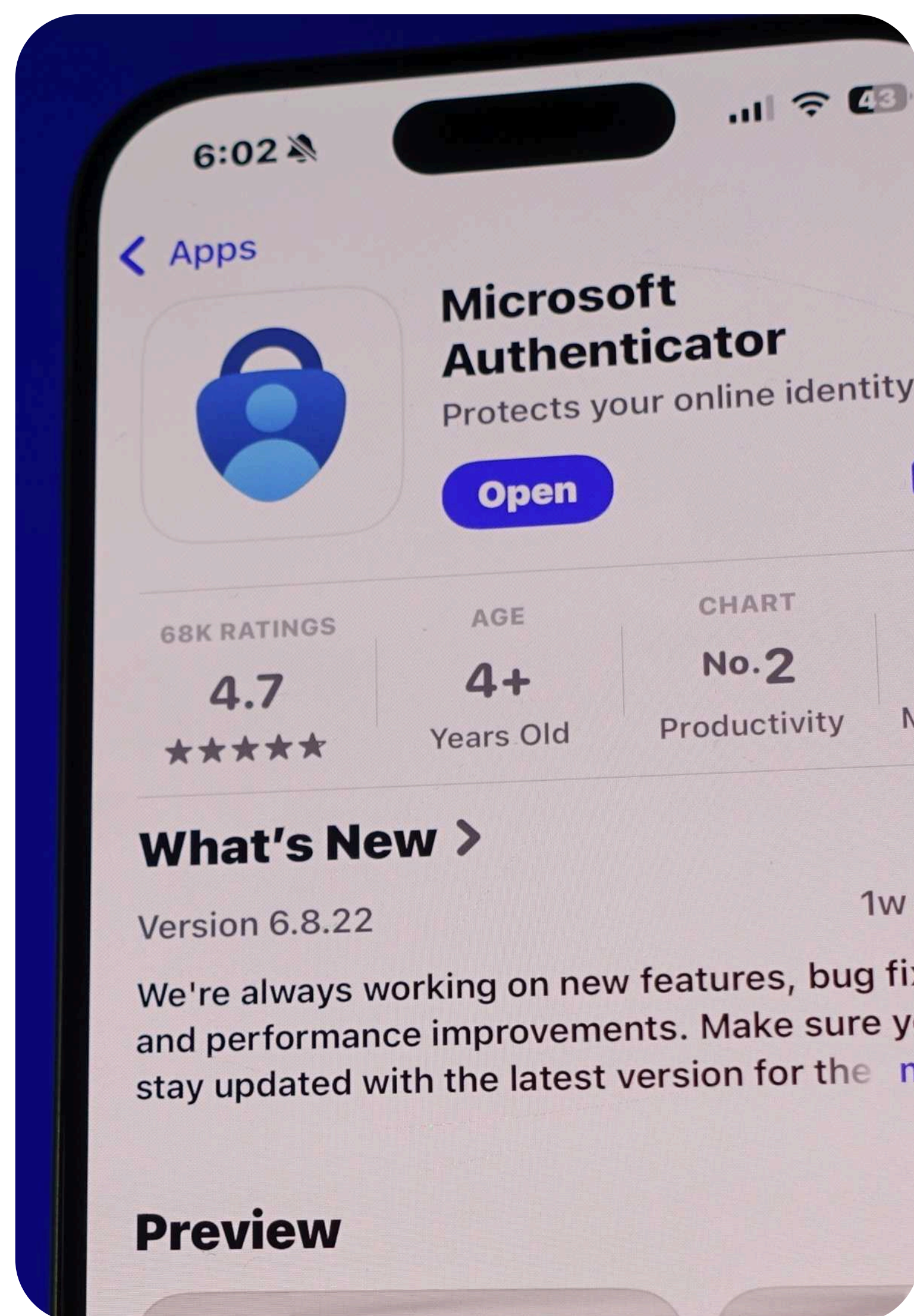


W Polsce od 2018 roku funkcjonuje Węzeł Krajowy (login.gov.pl) integrujący systemy usługowe administracji, m.in. ePUAP, biznes.gov.pl, pacjent.gov.pl, portale CEIDG i PUE ZUS oraz wiele innych z jednostek centralnych oraz samorządu terytorialnego. Dostęp do usług przez Węzeł Krajowy pozwala używać uniwersalnego loginu i bezpiecznego hasła oraz korzystać z różnych środków identyfikacji elektronicznej oraz identyfikować użytkowników w oparciu o Profil Zaufany będący bezpiecznym środkiem identyfikacji elektronicznej.



Kolejnym zestawem narzędzi wykorzystywanych w procedurach uwierzytelnienia są oferowane przez różne podmioty autentykatory, czyli aplikacje uwierzytelniające, uruchamiane przez użytkownika, generujące i przechowujące zestawy jednorazowych, zmienianych cyklicznie haseł.

Do najpopularniejszych obecnie autentykatorów należą: Google Authenticator i Microsoft Authenticator.



Autoryzacja użytkownika

Autoryzacja to proces zarządzania uprawnieniami dostępu do zasobów i przetwarzania informacji przez zidentyfikowanego wcześniej użytkownika. Zadaniem administratora (dostawcy usługi) jest zapewnienie właściwego przydziału uprawnień w zależności od roli, zadanych celów działania oraz zakresu obowiązków lub ustaleń kontraktowych dotyczących konkretnego użytkownika. Dostęp do zasobów przetwarzanych w systemie może odbywać się w różnych trybach i zakresach (odczyt, zapis, odczyt

i zapis, pobieranie, przesyłanie, podgląd częściowy z maskowaniem danych, zlecenie czynności lub ich aktywowanie itp.). Obowiązywać powinna zasada „Need-to-know!”, czyli zasada wiedzy niezbędnej, z której należy wywodzić zakres koniecznych uprawnień. Dobrą praktyką jest zbudowanie macierzy uprawnień i przyporządkowywanie użytkowników do uwzględnionych w niej zestawów przywilejów. Ważnym elementem zarządzania uprawnieniami jest usuwanie uprawnień nadmiarowych, które nie są już potrzebne lub nie są należne użytkownikowi ze względu na zmiany związane z jego aktywnością i przywilejami. Zarządzanie zmianą powinno odbywać się na podstawie odpowiednio przygotowanych procedur, których realizację należy dokumentować. Zasadą powinno być konsultowanie przydziału uprawnień z właścicielami biznesowymi poszczególnych zasobów lub procesów, aby dostępy były przydzielane zgodnie z wymogami i przyjętymi regułami bezpieczeństwa.

Rozliczalność procesów

Wszystkie istotne operacje w systemach informatycznych (w szczególności logowanie się użytkowników i dostęp do poszczególnych zasobów) powinny być rejestrowane, aby było możliwe sprawdzenie, czy przetwarzania dokonywały wyłącznie osoby upoważnione i czy odbywało się to zgodnie z ich uprawnieniami i założonymi zasadami przetwarzania oraz czy nie dochodziło do ewentualnych nadużyć, wynikających z błędów lub aktywności użytkowników albo błędnych parametrów lub konfiguracji nadzorowanych procesów. Zaleca się wdrożenie mechanizmów pozwalających na kompleksową analizę logów systemowych i operacji w poszczególnych modułach aplikacyjnych i zasobach, aby zapewnić systematyczną kontrolę przetwarzania informacji oraz możliwość wykazania kto, kiedy, w jakim celu oraz w jaki sposób przetwarzał dane. Celem jest tu wsparcie dokumentowania i rozliczalność procesów.

Mając na uwadze zmiany w dostępnych technologiach, rozwój rozwiązań oraz wzrost zagrożeń, administrator powinien zadbać o różny, dostosowany do istotności oraz ryzyka, poziom

bezpieczeństwa dla różnych grup użytkowników i administratorów w systemach przetwarzających dane. Ważne jest utrzymanie wysokich standardów kontroli dostępu do zasobów, zgodnie z przyjętym modelem i zasadami postępowania. Szczególnym nadzorem i niezwłoczną reakcją powinny zostać objęte wszelkie stwierdzone zaniedbania w zakresie stosowanych mechanizmów identyfikujących i dopuszczających użytkowników do systemów. Należy niezwłocznie eliminować błędy w tym zakresie, ponieważ kompromisy i brak reakcji mogą doprowadzić do incydentów związanych z bezpieczeństwem informacji lub ochroną przetwarzanych danych.

Możliwość audytu

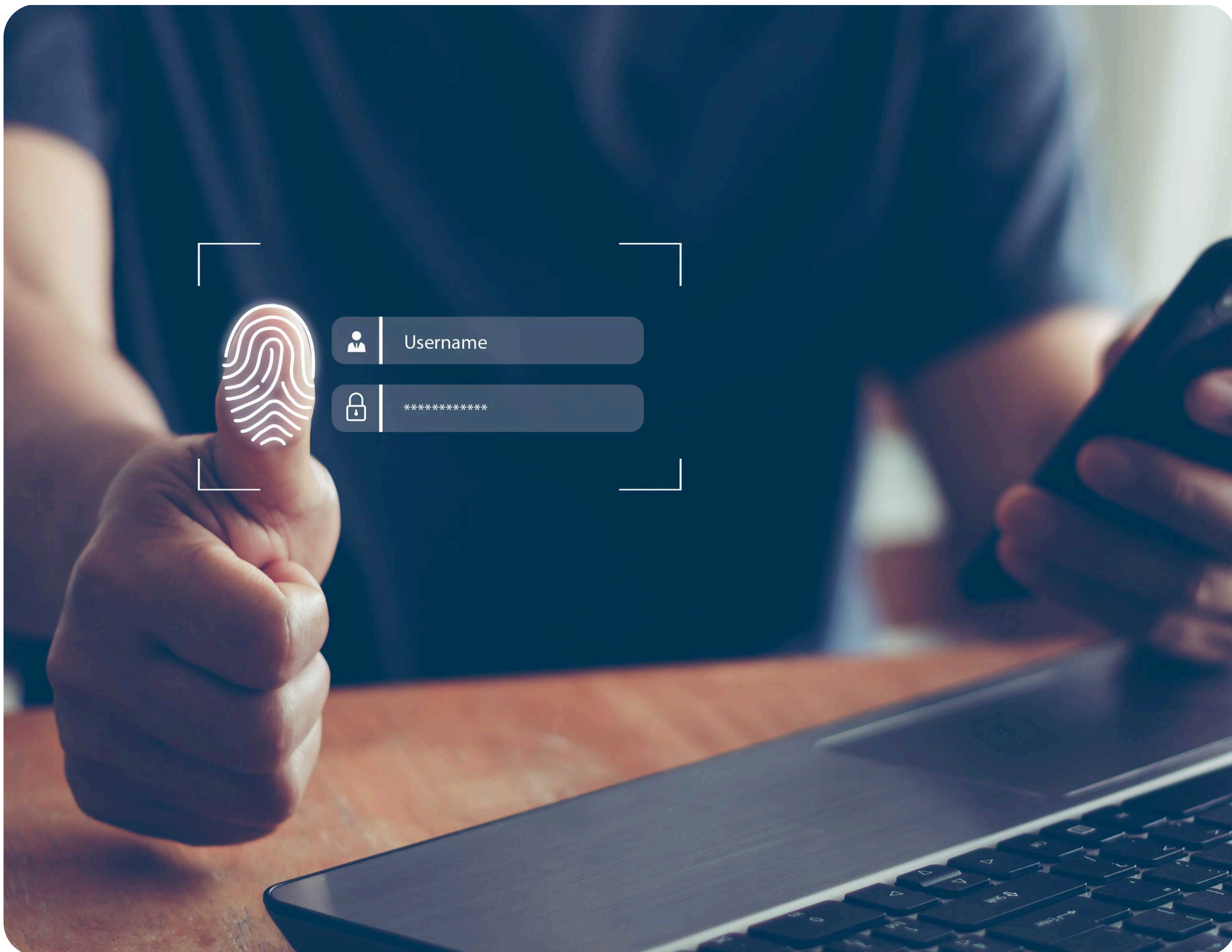
Jednym z elementów profesjonalnego procesu nadzoru nad funkcjonowaniem systemów, w których są przetwarzane dane, jest możliwość niezależnego sprawdzenia czy wszystkie procesy, począwszy od logowania się użytkowników i udzielania im dostępu do zasobów, przez zarządzanie przetwarzaniem pojemnością, wydajnością i bezpieczeństwem danych, po etap niszczenia informacji, funkcjonują poprawnie.

Wprowadze analizy takie są wykonywane również w ramach rozliczalności procesów, ale mając na uwadze specyfikę pracy operacyjnej, dużą ilość danych, które mogą ulegać modyfikacjom oraz ryzyko usunięcia niektórych informacji zaleca się wdrożyć rozwiązania zapewniające możliwość niezależnego kontrolowania poprawności całego procesu i jakości informacji diagnostycznych i raportowych w oparciu o powielone i odseparowane kopie informacji posiadające atrybut niezaprzeczalności dla zebranych i odpowiednio zagregowanych dowodów audytowych.

Podsumowanie

O tym, jak ważne jest właściwe zarządzanie identyfikacją użytkowników i przyznawanymi im uprawnieniami można przekonać się, gdy dojdzie do zakłóceń w tych procesach i osoby, aplikacje, systemy lub urządzenia nieupoważnione uzyskają dostęp do danych dla siebie nieprzeznaczonych. Skutki takich incydentów mogą mieć negatywny wpływ (organizacyjny, prawny, finansowy i wizerunkowy) na podmioty odpowiedzialne za ochronę przetwarzanych informacji, które nie dochowały należytej staranności dotyczącej zasad dostępu do zasobów. Dlatego zaleca się aby każdy dysponent danych, kontrolując i zestawiając informacje z modelu AAA: „Kto?”, „Do czego jest uprawniony?” i „Co robił?”, zapewniał należyty nadzór nad przetwarzanymi przez użytkowników zasobami i dbał, aby dostęp do nich był możliwy jedynie dla zweryfikowanych, uprawnionych i odpowiednio umocowanych do działania użytkowników, a użyte rozwiązania w sposób optymalny wspierały i zapewniały adekwatną ochronę, na wymaganym przez dysponenta danych poziomie.





Newsletter RODO

Marzec 2025 nr 3/2025

Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

[SKONTAKTUJ SIĘ Z NAMI](#)