

1. WYMAGANIA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

1.1. Wstęp

W przypadku gdy dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Wykonawca przed odbiorem końcowym i przed rozpoczęciem przetwarzania przez Zamawiającego dokona oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (DPIA). Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Analizując poprawność przetwarzania danych osobowych w systemie można posłużyć się tabelą z punktu 1.11

Wszystkie procesy nadzorujące muszą być zautomatyzowane i dostępne z poziomu upoważnionego użytkownika. System powinien umożliwiać generowanie informacji wymaganych przepisami prawa z zakresu ochrony danych osobowych (np. art. 13 lub 14 RODO) oraz zapewniać mechanizmy rozliczalności pozwalających na wykazanie ich przestrzeganie obowiązków z zakresu informowania podmiotów zasadach przetwarzania ich danych osobowych.

1.2. Wymagania prawne

System spełnia pod względem prawnym wymagania przepisów o ochronie danych osobowych (krajowych, jak i Unii Europejskiej), w szczególności:

1. 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 (ogólne rozporządzenie o ochronie danych), dalej również RODO,
2. ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (u.o.d.o)
3. ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jednolity Dz. U. z 2014 r. poz. 1114) oraz wydane do niej rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jednolity Dz. U. z 2016 r. poz. 113)."

1.3. Ogólne wymagania dotyczące bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym

1. Jeżeli dane osobowe przetwarzane są bezpośrednio w systemie:
 - a. dane w spoczynku (z ang. data at rest) są szyfrowane zgodnie z aktualnymi standardami i zgodnie z wymogami stawianymi w art. 32 ust. 1 RODO (min. AES-256),
 - b. dane w przesyśle (z ang. data-in-transfer) w zakresie w jakim transfer odbywa się poza infrastrukturę informatyczną administratora – szyfrowane są zgodnie z aktualnymi standardami i zgodnie z wymogami stawianymi w art. 32 ust. 1 RODO (min. AES-256).
 - c. system umożliwi stosowanie metod pseudonimizacji danych – szczegółowe metody pseudoanonimizacji zostaną określone w analizie wdrożeniowej.

2. Jeżeli dane osobowe przechowywane są poza systemem system umożliwia (z uwzględnieniem rynkowych standardów) szyfrowanie danych w przesyłce (data-in-transfer) pomiędzy systemem a źródłem (np. bazą danych) z którego są one pobierane i do którego są one zapisywane.
3. System ma zdolność do ciągłego zapewnienia: poufności, integralności, dostępności i odporności systemów i usług przetwarzania.
4. System ma zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego (w szczególności przez automatyczne backupy).
5. System zapewnia rozliczalność dokonywanych w nim operacji na danych, w szczególności system rejestruje (np. w logach) wykonywanie operacji na danych osobowych i umożliwia wskazanie przypisania operacji do konkretnego konta w systemie.
6. System zabezpiecza logi przed nieautoryzowanym dostępem, modyfikacją lub usunięciem przez okres zgodny z ustalonymi zasadami bezpieczeństwa.

1.4. Ogólne wymagania dotyczące bezpieczeństwa przetwarzania danych osobowych w chmurze obliczeniowej (w części systemu działającego w środowisku chmurowym)

1. Wykorzystywana przez System chmura obliczeniowa musi zapewniać zgodność z zapisami RODO w kwestii przetwarzania danych oraz wymagane jest, aby dane były przechowywane na terenie EOG z możliwością kontroli tego procesu .
2. System powinien zapewnić, że informacje przetwarzane w chmurze obliczeniowej są szyfrowane zgodnie z poniższymi zasadami:
 - a) Zamawiający posiada dostęp do szczegółowych i aktualnych instrukcji konfiguracji usług chmury obliczeniowej oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji.
 - b) Przetwarzanie danych będzie odbywało się w poprawnej konfiguracji usług chmury obliczeniowej, a jeżeli usługi chmurowe będą świadczone przez podmiot trzeci - zgodnie z wytycznymi dostawcy usług chmury obliczeniowej, w tym pod kątem stosowania szyfrowania przetwarzanych informacji;
 - c) informacje prawnie chronione przetwarzane w chmurze obliczeniowej są szyfrowane zarówno „data at rest” jak i „data in transit” na zasadach co najmniej określonych w pkt 3.1.
 - d) Informacje są szyfrowane kluczami generowanymi przez Zamawiającego lub przez niego zarządzane, chyba że z oszacowania ryzyka wynika, wyniknie iż dopuszczalne lub wskazane jest używanie kluczy szyfrujących generowanych lub zarządzanych przez Wykonawcę lub dostawcę usług chmury obliczeniowej.
 - e) W przypadku, gdy z szacowania ryzyka wynika konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu sprzętowych rozwiązań (HSM9), to HSM mogą być udostępniane przez dostawcę usług chmury obliczeniowej, przy uwzględnieniu tego elementu w szacowaniu ryzyka. HSM powinny spełniać wymagania minimum FIPS10 140-2 Level 2 lub równoważne.
 - f) Proces zarządzania kluczami szyfrującymi powinien uwzględniać przechowywanie w ramach własnej infrastruktury kopii kluczy szyfrujących, które zostały wygenerowane lub są zarządzane przez dostawcę usług chmury obliczeniowej, chyba że z oszacowania ryzyka wynika uzasadniony brak takiej potrzeby.
 - g) System zabezpiecza logi przed nieautoryzowanym dostępem, modyfikacją lub usunięciem przez okres zgodny z ustalonymi zasadami bezpieczeństwa.

1.5. Zarządzanie uprawnieniami użytkowników systemu w zakresie dostępu do danych osobowych

1. System powinien wyodrębniać poszczególne kategorie predefiniowanych danych (np. imię i nazwisko, adres, PESEL) i umożliwiać dostosowanie do których kategorii danych ma dostęp dany użytkownik. Zakres predefiniowanych danych zostanie uzgodniony i zaakceptowany przez Zamawiającego w trakcie analizy systemowej.
2. System powinien umożliwiać tworzenie lub posiadać predefiniowane grupy użytkowników (np. pracownicy, kierownicy, dyrektorzy) w stosunku do których można dostosować do których kategorii danych grupa ma dostęp; Zakres predefiniowanych grup użytkowników oraz ewentualne zmiany zostaną uzgodnione i zaakceptowane przez Zamawiającego w trakcie analizy systemowej.

Z zastrzeżeniem, że Zamawiający oczekuje, że zakres dostępu do danych przez użytkownika w systemie, będzie odpowiadał organizacji pracy u Zamawiającego, jednocześnie Zamawiający biorąc pod uwagę zgłaszany problem postara się dostosować organizację pracy do funkcjonalności systemu. W skrajnych przypadkach Zamawiający pozostawia sobie prawo do wymagania od dostawcy modyfikacji w przedmiotowym zakresie. Zakres ewentualnych zmian zostanie uzgodniony w trakcie analizy systemowej.

1.6. Przepływ danych osobowych – mapa procesów systemu

1. System powinien mieć zmapowane wszystkie procesy, w ramach których dochodzi do przetwarzania danych osobowych w systemie.
2. Mapa procesów systemu powinna wskazywać co najmniej przepływ kategorii danych (np. imię nazwisko, adres, PESEL) w danym procesie.

1.7. Raporty i wydruki generowane przez system w zakresie ochrony danych osobowych

1. System generuje raporty obrazujące jakiego zakresu zmian dokonano, wartość początkową i wartość końcową ze wskazaniem użytkownika i czynności, która została przeprowadzona.
2. System generuje raporty rekordów danych przetwarzanych na podstawie zgody, funkcjonalność wymagana w przypadku, gdy w trakcie analizy systemowej wskazane zostają dane przetwarzane w systemie na podstawie zgody.
3. System generuje raporty rekordów danych, dla których wycofano zgodę na przetwarzanie danych, funkcjonalność wymagana w przypadku, gdy w trakcie analizy systemowej wskazane zostają dane przetwarzane w systemie na podstawie zgody. .
4. System generuje raporty dla rekordów danych, których czas retencji minął, przy czym Zamawiający dopuszcza w wypadku, gdy wymaganie te nie stanowi automatycznego narzędzia systemu, aby zostało zrealizowane na każde żądanie Zamawiającego przez Wykonawcę w ramach Usług Utrzymania.
5. System generuje raporty dotyczące żądań podmiotów danych praw art. 1615-18 oraz 20-22, albo ograniczenie UODO z art. 58 ust.2 lit.f RODO.
6. System generuje raporty o przekazaniu informacji, o których mowa w pkt 2 dla potrzeb rozliczalności, funkcjonalność wymagana w przypadku, gdy w trakcie analizy systemowej wskazane zostają dane przetwarzane w systemie na podstawie zgody.

1.8. Kopie danych / backupy danych osobowych

1. System umożliwia odtworzenie danych i konfiguracji systemu w dowolnym punkcie w czasie.
2. Backupy powinny obejmować także informacje o logach
3. W trakcie Analizy Systemowej Wykonawca przedstawi sposób realizacji wymagań 1-2.

1.9. Retencja danych osobowych

1. System umożliwia usunięcie danych, których czas retencji minął
2. System umożliwia oznaczenie (tagowanie, oflagowanie) rekordów danych dotyczących osób, których czas retencji minął. Oznaczanie skutkuje automatycznym (realizowanym przez system) wykluczeniem oznaczonych danych ze „zwykłych operacji”.
3. System umożliwia usunięcie danych, których czas retencji minął.
4. System powiadamia użytkownika o upływie czasu retencji danych.
5. Sposób spełnienia wymagań w zakresie retencji danych, o których mowa w pkt 1-4 powyżej zostanie opracowany przez wykonawcę na etapie Analizy Systemowej, przy czym Zamawiający dopuszcza w wypadku, gdy wymagania 1-3 te nie stanowią automatycznego narzędzia systemu, aby zostały zrealizowane przez Wykonawcę w ramach Usług Utrzymania”;

1.10. Wymagania funkcjonalne związane z realizacją w systemie praw osoby której dane dotyczą, o których mowa w art. 7 oraz art. 15 do art. 22 RODO w szczególności. rejestracji zgody i cofnięcia zgody, do usunięcia danych, sprzeciwu, sprostowania, ograniczenia dostępu do danych, informacji o przetwarzaniu, kopii danych)

1. System umożliwia oznaczenie (tagowanie, oflagowanie) rekordów danych dotyczących osób, których przetwarzanie odbywa się na podstawie zgody, funkcjonalność wymagana w przypadku, gdy w trakcie Analizy Systemowej wskazane zostają dane przetwarzane w systemie na podstawie zgody .
2. W przypadku cofnięcia zgody na przetwarzanie danych takie oznaczenie skutkuje powiadomieniem użytkownika, że dane można przechowywać, ale nie należy ich tymczasowo używać w „zwykłych operacjach” funkcjonalność wymagana w przypadku, gdy w trakcie Analizy Systemowej wskazane zostają dane przetwarzane w systemie na podstawie zgody. .
3. W przypadku cofnięcia zgody na przetwarzanie danych takie oznaczenie skutkuje automatycznym (realizowanym przez system) wykluczeniem oznaczonych danych ze „zwykłych operacji” funkcjonalność wymagana w przypadku, gdy w trakcie Analizy Systemowej wskazane zostają dane przetwarzane w systemie na podstawie zgody. .
4. Jeżeli system przetwarza dane osobowe w różnych celach to jest tego świadomy i implementuje lub umożliwia oznaczanie danych w oparciu o konkretne cele przetwarzania; takie oznaczenie ma swoje logiczne konsekwencje dla możliwych czynności przetwarzania oraz realizacji praw osób.
5. System umożliwia wyszukanie osoby wg określonego zestawu atrybutów, w szczególności wg unikalnych identyfikatorów jeśli występują w systemie; prezentacja wyników wyszukiwania odbywa się „po jednym rekordzie” albo tylko w przypadku znalezienia jednego rekordu w wyniku zastosowania kryteriów wyszukiwania.
6. . System umożliwia (w wyniku wywołania wbudowanej w niego funkcjonalności) eksportowanie danych dotyczących konkretnej osoby w jednym z następujących formatów danych: txt, csv, xml, json, przeszukiwany i edytowalny pdf. Dopuszczalne jest wielokrotne wywołanie funkcjonalności w celu otrzymania kompletu danych, oczekiwane jest jednokrotne wywołanie skutkujące kompletem danych.
7. .

1.11. Lista sprawdzająca poprawność przetwarzania danych osobowych w systemie

	Podstawa prawna wynikająca z RODO	Zagadnienia/Wymogi przy wdrażaniu nowego procesu (aplikacji)	TAK	NIE	NIE DOTYCZY	Uwagi
1.	Art. 4 pkt 1)	W ramach procesu przetwarzane są dane osobowe;				
2.	Art. 9 ust. 1	W ramach procesu przetwarzane są dane osobowe szczególnej kategorii; <i>(są to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby).</i>				
3.	Art. 10	Przetwarzane są dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa;				
4.	Art. 4 pkt 1)	Aby korzystać z aplikacji konieczne jest podanie danych osobowych;				
5.	Art. 5 ust.1 lit. a), Art. 6 ust. 1, Art. 9 ust. 2	Przetwarzanie odbywa się zgodnie z prawem – ustalono przesłanki legitymujące przetwarzanie danych osobowych w każdym z celów, jaki ma być realizowany w związku z funkcjonowaniem aplikacji;				
5a.	Art. 6	Przetwarzanie danych zwykłych ma podstawę prawną;				
5b.	Art. 6, Art. 9	Przetwarzanie danych szczególnej kategorii ma podstawę prawną;				

5c.	Art. 6, Art. 10	Przetwarzanie danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa ma podstawę prawną oraz odbywa się pod nadzorem władz publicznych lub jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą;				
6.	Art. 5 ust. 1 lit. a), Art. 6 ust. 1 lit. a), Art. 9 ust. 2 lit. a)	Przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą;				
6a.	Art. 5 ust. 1 lit. a), Art. 9 ust. 2 lit. a)	Przetwarzanie danych osobowych szczególnych kategorii odbywa się na podstawie wyraźnej zgody osoby, której dane dotyczą;				
6b.	Art. 5 ust. 1 lit. a), Art. 5 ust. 2, Art. 7 ust. 1	Administrator jest w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub kilku konkretnych celach przetwarzania danych;				
6c.	Art. 5 ust. 1 lit. a), Art. 5 ust. 2, Art. 7 ust. 2	Jeżeli zgoda wyrażana jest w pisemnym oświadczeniu, które dotyczy także innych kwestii – zapytanie o zgodę jest przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;				
6d.	Art. 5 ust. 1 lit. a), Art. 7 ust. 3	Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę;				
6e.	Art. 5 ust. 1 lit. a), Art. 7 ust. 3	Osoba, której dane dotyczą, jest informowana o możliwości wycofania zgody, zanim wyrazi tę zgodę;				
6f.	Art. 5 ust. 1 lit. a), Art. 7 ust. 4	Wyrażenie zgody na przetwarzanie danych jest w pełni dobrowolne – brak jej wyrażenia nie ma negatywnych konsekwencji dla osoby, której dane dotyczą;				
7.	Art. 5 ust. 1 lit. a), Art. 6 ust. 1 lit. f)	Przetwarzanie odbywa się jako niezbędne dla realizacji prawnie uzasadnionych interesów administratora lub strony trzeciej (na podstawie tej przesłanki może się odbywać wyłącznie				

		przetwarzanie danych osobowych zwykłych);				
7a.	Art. 5 ust. 1 lit. a), Art. 6 ust. 1 lit. f)	Przeprowadzono test ważenia interesów (bilansujący), który wykazał, że po stronie administratora lub strony trzeciej istnieją interesy w przetwarzaniu danych osobowych nadrzędne względem interesów osób, których dane dotyczą;				
7b.	Art. 5 ust. 1 lit. a), Art. 6 ust. 1 lit. f), Art. 21	Umożliwiono osobie, której dane dotyczą, złożenie sprzeciwu wobec przetwarzania dotyczących jej danych osobowych na podstawie art. 6 ust. 1 lit. e) oraz f) RODO.				
7c.	Art. 5 ust. 1 lit. a), Art. 6 ust. 1 lit. f), Art. 21 ust. 2	Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą może w dowolnym czasie wnieść sprzeciw wobec przetwarzania jej danych.				
8.	Art. 8 ust. 1	Aplikacja jest wykorzystywana do świadczenia usług społeczeństwa informacyjnego				
8a.	Art. 5 ust. 1 lit. a), Art. 8 ust. 1	Dane przetwarzane są na podstawie zgody w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, które nie ukończyło 16 lat.				
8b.	Art. 5 ust. 1 lit. a), Art. 8 ust. 1	Jeżeli w 8a odpowiedziano „tak”, to: Przetwarzanie odbywa się na podstawie zgody wyrażonej przez osobę sprawującą władzę rodzicielską lub opiekę nad dzieckiem;				
9.	Art. 5 ust. 1 lit. a), Art. 12, Art. 13, Art. 14	Dane są przetwarzane w sposób rzetelny i przejrzysty dla osoby, której dane dotyczą – ustalono zasady informowania o przetwarzaniu i komunikacji z osobą, której dane dotyczą;				
9a.	Art. 5 ust. 1 lit. a), Art. 12, Art. 13, Art. 14	Wobec osób, których dane osobowe są przetwarzane w aplikacji został spełniony/zostanie spełniony obowiązek informacyjny wynikający z art. 13 lub 14 RODO;				
9b.	Art. 5 ust. 1 lit. a), Art. 12, Art. 13, Art. 14	Użytkownik aplikacji na każdym etapie przetwarzania danych może zapoznać się z zasadami przetwarzania danych osobowych np. dzięki odwołaniu do Polityki Prywatności;				

10.	Art. 5 ust. 1 lit. a)	Osoby, których dane dotyczą, zostały poinformowane o dotyczących je prawach oraz sposobach ich egzekwowania od administratora, kanałach komunikacji z administratorem, wymogów dotyczących wniosków i żądań;				
11.	Art. 5 ust. 1 lit. a), Art. 15	Umożliwiono osobom, których dane dotyczą, dostęp do dotyczących ich danych osobowych. Osoba, której dane dotyczą może uzyskać od administratora potwierdzenie, czy przetwarzane są dane jej dotyczące, a jeśli ma to miejsce może uzyskać informacje dotyczącego tego przetwarzania;				
12.	Art. 5 ust. 1 lit. a), Art. 15 ust. 3	Umożliwiono osobom, których dane dotyczą, uzyskanie kopii dotyczących ich danych osobowych.				
13.	Art. 5 ust. 1 lit. b)	Sprecyzowano cele przetwarzania danych – dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; <i>(dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami);</i>				
13a.	Art. 5 ust. 1 lit. b), Art. 6 ust. 4	Jeżeli dane wykorzystywane przez aplikację zostały pierwotnie zebrane w innym procesie niż związany z funkcjonowaniem aplikacji – przeprowadzono test zgodności celów przetwarzania i otrzymano pozytywny wynik w zakresie zgodności celów przetwarzania;				

13b.	Art. 5 ust. 1 lit. b), Art. 6 ust. 4	Jeżeli dane wykorzystywane przez aplikację zostały pierwotnie zebrane w innym procesie niż związany z funkcjonowaniem aplikacji i na 13a odpowiedziano „nie”, to: pozyskano zgodę osoby, której dane dotyczą, na przetwarzanie jej danych w celu innym niż pierwotny cel przetwarzania lub konieczność przetwarzania wynika z prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, m.in. bezpieczeństwu narodowemu, obronie, bezpieczeństwu publicznemu, zapobieganiu przestępczości, innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu, funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej, ochronie osoby, której dane dotyczą, lub praw i wolności innych osób, egzekucji roszczeń cywilnoprawnych.				
14.	Art. 5 ust. 1 lit. c), Art. 25	Dane przetwarzane w aplikacji są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;				
15.	Art. 5 ust. 1 lit. d)	Dane są i mogą być w razie potrzeby uaktualniane;				
16.	Art. 5 ust. 1 lit. d)	Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostają niezwłocznie usunięte lub sprostowane;				
17.	Art. 5 ust. 1 lit. d), Art. 16	Umożliwiono osobom, których dane dotyczą, sprostowanie swoich danych. Na żądanie osoby, której dane dotyczą nieprawidłowe dane są niezwłocznie sprostowane;				

18.	Art. 5 ust. 1 lit. e)	Dane przechowywane są przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; <i>(dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą);</i>				
19.	Art. 5 ust. 1 lit. e), Art. 17	Umożliwiono osobom, których dane dotyczą, złożenie żądania usunięcia ich danych osobowych. Na żądanie osoby, której dane dotyczą dane mogą być usuwane, o ile przepisy prawa pozwolą na usunięcie tych danych;				
20.	Art. 5 ust. 1 lit. e), Art. 18	Umożliwiono osobom, których dane dotyczą, złożenie żądania ograniczenia przetwarzania ich danych osobowych. Na żądanie osoby, której dane dotyczą zakres przetwarzanych danych może zostać ograniczony, o ile przepisy prawa pozwolą na takie ograniczenie przetwarzania tych danych;				
21.	Art. 20	Dane mogą być wyeksportowane z aplikacji;				
22.	Art. 20	Umożliwiono osobom, których dane dotyczą, złożenie żądania przenoszenia ich danych osobowych. Na żądanie osoby, której dane dotyczą dane mogą być przenoszone, o ile przepisy prawa pozwolą na takie ograniczenie przetwarzania tych danych;				
23.	Art. 5 ust. 2	Aplikacja pozwala na generowanie raportów dotyczących eksportów danych z aplikacji, w tym zawierających informacje o czasie eksportu i ewentualnym adresacie danych;				
24.	Art. 22 ust. 1	Czy osoba, której dane są przetwarzane podlega decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu?				
25.	Art. 22 ust. 1	Czy profilowaniu podlegają również dane szczególnej kategorii?				

26.	Art. 22 ust. 1	Czy zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w 24, wywołuje wobec tej osoby, której dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływa?				
27.	Art. 5 ust. 1 lit. f), Art. 32	Przeprowadzono stosowną analizę ryzyka naruszenia praw i wolności osób, których dane dotyczą, w związku z przetwarzaniem ich danych w ramach aplikacji				
28.	Art. 35	Dany rodzaj przetwarzania danych, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. <i>(Jeżeli tak - administrator przed rozpoczęciem przetwarzania musi dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych);</i>				
29.	Art. 5 ust. 1 lit. f), Art. 35	Przeprowadzono ocenę skutków przetwarzania danych w ramach aplikacji dla ochrony danych osobowych.				
30.	Art. 36	Ocena skutków dla ochrony danych, wykazała, że przetwarzanie powodowałoby wysokie ryzyko – jednocześnie nie zastosowano środków w celu zminimalizowania tego ryzyka. <i>(Jeżeli tak – administrator przed rozpoczęciem przetwarzania konsultuje się z organem nadzorczym);</i>				
31.	Art. 5 ust. 1 lit. f), Art. 36	Przeprowadzono uprzednie konsultacje z organem nadzorczym/osobami, których dane dotyczą/IOD				
32.	Art. 5 ust. 1 lit. f), Art. 32	Wdrożono, odpowiednie – ze względu na poziom ryzyka – środki techniczne i organizacyjne, zapewniające właściwy stopień bezpieczeństwa przetwarzania, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;				

33.	Art. 5 ust. 1 lit. f), Art. 26	Przetwarzanie danych w ramach procesu zlecane jest realizowane we współpracy z innym administratorem, w ramach wspólnego podejmowania decyzji o celach i sposobach przetwarzania (współadministracja)				
33a.	Art. 5 ust. 1 lit. f), Art. 26	Jeżeli odpowiedź na 33. to „tak”, to: ze współadministratorem zawarto porozumienie o współadministrowaniu danymi osobowymi;				
33b.	Art. 5 ust. 1 lit. f), Art. 26	Jeżeli odpowiedź na 33. to „tak”, to: ustalono brzmienie informacji opisującej zasadniczą część uzgodnień współadministratorów i sposób komunikowania zasadniczej części uzgodnień współadministratorów osobom, których dane dotyczą;				
33c.	Art. 5 ust. 1 lit. f), Art. 26	Jeżeli odpowiedź na 33. to „tak”, to: ustalono punkt kontaktowy dla osób, których dane dotyczą;				
34.	Art. 5 ust. 1 lit. f), Art. 28	Przetwarzanie danych w ramach procesu zlecane jest podmiotom trzecim (firmom zewnętrznym).				
34a.	Art. 5 ust. 1 lit. f), Art. 28	Jeżeli odpowiedź na 34. to „tak”, to: podmioty przetwarzające zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą – przeprowadzono wstępną weryfikację procesora;				
34b.	Art. 5 ust. 1 lit. f), Art. 28	Jeżeli odpowiedź na 34. to „tak”, to: z podmiotem przetwarzającym zawarto/planuje się zawrzeć umowę powierzenia;				
35.	Art. 5 ust. 1 lit. f), Art. 29	Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora (chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego);				
36.	Art. 5 ust. 1 lit. a), Art.	Dane są przekazywane poza Europejski Obszar Gospodarczy.				

	45 i nast.					
36a.	Art. 5 ust. 1 lit. a), Art. 45 i nast.	Jeżeli odpowiedź na 36. to „tak”, to: Dane przekazywane są na podstawie decyzji stwierdzającej, że państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony;				
36b.	Art. 5 ust. 1 lit. a), Art. 45 i nast.	Jeżeli odpowiedź na 36. to „tak” a na 36a. to „nie”, to: wykonano analizę skutków transferu dla ochrony danych osobowych oraz praw i wolności osób, których dane dotyczą (tzw. transfer impact assessment);				
36c.	Art. 5 ust. 1 lit. a), Art. 45 i nast.	Jeżeli odpowiedź na 36. to „tak” a na 36a. to „nie”, to: Dane przekazywane są na podstawie innego instrumentu prawnego, np. na podstawie standardowych klauzul umownych przyjętych przez Komisję (art. 46 ust. 2 lit. c) RODO) lub standardowych klauzul umownych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję (art. 46 ust. 2 lit. d) RODO);				
36d.	Art. 5 ust. 1 lit. a), Art. 45 i nast.	Jeżeli odpowiedź na 36. to „tak” a na 36a. to „nie”, to: Dane są przekazywane na podstawie zatwierdzonego kodeksu postępowania lub mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami ADO lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w szczególności w odniesieniu do praw osób, których dane dotyczą;				
36e.	Art. 5 ust. 1 lit. a), Art. 45 i nast.	Jeżeli odpowiedź na 36. to „tak” a na 36a. i 36b. to „nie”, to: Dane są przekazywane na podstawie decyzji wydanej przez organ nadzorczy, która nie została zmieniona, zastąpiona lub uchylona;				
36f.	Art. 5 ust. 1 lit. a), Art. 45 i nast.	Jeżeli odpowiedź na 36. to „tak” a na 36a – 36e to „nie”, to: Dane przekazywane są na podstawie jednego z wyjątków z art. 49 RODO, to jest m.in.: na podstawie zgody, osoby, której dane dotyczą, która została poinformowana o ewentualnym ryzyku transferu, lub gdy przekazanie jest niezbędne ze względu na				

		ważne względy interesu publicznego;				
--	--	-------------------------------------	--	--	--	--