ZAŁĄCZNIK 2

**Wymagania RODO dotyczące systemów informatycznych, w których przetwarzane są dane osobowe**

Funkcjonalności, w jakie powinien być wyposażony system informatyczny. w którym przetwarzane są dane osobowe:

1. Funkcjonalność umożliwiająca usuwanie/anonimizację danych osobowych w nim zawartych, z możliwością anonimizacji/usunięcia zarówno jednego, jak i wielu rekordów jednocześnie.
2. Mechanizm umożliwiający generowanie i drukowanie – dla każdej osoby, której dane osobowe są przetwarzane – raportu zawierającego zakres przetwarzanych danych oraz informacje o dacie pierwszego wprowadzenia danych i kolejnych aktualizacjach, a także o operatorach wprowadzających i zmieniających dane z datą i godzina ich dokonania.
3. Funkcjonalność umożliwiająca rejestrację sprzeciwu osoby w zakresie przetwarzania jej danych osobowych i trwałego oznaczenia takiego rekordu z jednoczesną anonimizacją danych jej dotyczących. Zgłoszenie sprzeciwu musi być łatwo dostępne (np. poprzez formularz kontaktowy).
4. System informatyczny musi zapewniać możliwość tworzenia kopii zapasowych
(z możliwością szybkiego ich przywrócenia) i zapewniać ciągłość działania
w przypadku braku energii elektrycznej (UPS + Backup). Może to zostać zapewnione również przez dostawcę hostingu lub zewnętrznego administratora serwisu.
5. Mechanizm umożliwiający wysłanie wiadomości SMS lub mailowej zarówno do pojedynczych użytkowników, jak i do wybranej ich grupy.
6. System musi umożliwiać oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania (np. sprzeciw dotyczący przetwarzania
w celach marketingowych itd.).
7. System musi umożliwiać odnotowanie źródła pochodzenia danych, jeśli nie zostały one uzyskane od osoby, której dane dotyczą.
8. System musi umożliwiać odnotowanie informacji o odbiorcach, którym udostępniono dane.
9. Mechanizmy kontroli jakości danych (zabezpieczenia przeciw duplikowaniu danych, ew. inne mające wpływ na minimalizację ryzyka wpisania błędnych informacji, przykładowo, niemożność wpisania liter w pole, gdzie oczekiwany jest nr PESEL itp.).
10. System musi zapewniać rozliczalność (kto i kiedy modyfikował rekordy z danymi osobowymi) w odniesieniu do operacji dokonywanych na danych osobowych (to po części pokrywa się z pkt 2).
11. System powinien również umożliwiać łatwe uzyskanie informacji o danych kontaktowych osób administrujących serwisem, do których mogą zgłaszać np. żądanie poprawienia danych czy sprzeciw lub uzyskać informacje o ich danych przetwarzanych w systemie.
12. Oczywiście wszelkie połączenia w sieci publicznej, którymi przesyłane są dane dostępowe (hasła, loginy), powinny być szyfrowane jak dotąd.