**Wymogi dla systemów informatycznych służących do przetwarzania Danych Osobowych**

***Uwaga: Wypełnienie niniejszego kwestionariusza leży po stronie dostawcy systemu / oprogramowania wykorzystywanego do przetwarzania danych osobowych, lecz na część zawartych w nim pytań / zagadnień odpowiedzi udzielić musi również osoba administrująca systemem / oprogramowaniem po stronie Grupy Azoty (zwłaszcza w kontekście zabezpieczeń organizacyjnych, wykonywania kopii zapasowych itp.).***

Dla każdego systemu / oprogramowania przetwarzającego dane osobowe konieczna jest identyfikacja stosowanych obecnie i koniecznych do wdrożenia zabezpieczeń organizacyjnych i technicznych, wynikających z zapisów RODO[[1]](#footnote-1).

| Wymogi prawa w zakresie ochrony danych osobowych wynikające z RODO1 | | | |
| --- | --- | --- | --- |
| Lp. | **Wymaganie, źródło** | **System/ oprogramowanie spełnia wymaganie:**  **Tak/ Nie** | **Komentarze / uwagi osoby wypełniającej oraz Administratora systemu** |
|  | System zapewnia autoryzację użytkowników (art. 5 ust. 1, lit. f) |  | *Proszę o komentarz, w jaki sposób odbywa się autoryzacja użytkownika, czy system umożliwia dowolne definiowanie polityki haseł, proszę wskazać obowiązującą politykę haseł (złożoność hasła, długość, okres ważności, czy stosowanie polityki haseł „wymuszane” jest przez system itp.* |
|  | System zapewnia odrębny identyfikator rejestrowany dla każdego użytkownika (art. 5 ust. 2) |  | *Uwaga, system musi zapewniać rozliczalność przy zmianach identyfikatorów użytkowników systemów (np. zmiana identyfikatora przy zmianie nazwiska)* |
|  | Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie (art.5 ust. 2) |  | *Czy system posiada programowe zabezpieczenie przed rejestracją użytkownika o funkcjonującym już w systemie identyfikatorze? Czy opracowano procedurę zabezpieczającą przed przydzieleniem identyfikatora użytkownika, który utracił uprawnienia innej osobie?* |
|  | System zapewnia zabezpieczoną kryptograficznie transmisję danych (art.5 ust. 1 lit. f, art. 32 ust. 1 lit. a) |  | *Czy transmisja danych pomiędzy użytkownikiem i serwerem (jeżeli system działa w tego typu architekturze) zabezpieczona jest kryptograficznie? W przypadku systemów, z którymi komunikacja odbywa się za pośrednictwem przeglądarki internetowej transmisja jest zabezpieczona kryptograficznie?* |
|  | System zapewnia rozliczalność podejmowanych przez użytkownika działań - umożliwia jednoznaczne wskazanie, kto określone dane wprowadził lub zmieniał z podaniem dat operacji, system zapewnia pełną rozliczalność działań użytkownika podejmowanych w trakcie pracy w systemie (art. 5 ust. 2, art. 32 ust. 1, lit. b) |  | *Proszę o wskazanie, jakiego typu logi i jak długo przechowuje system* |
|  | System zapewnia możliwość raportowania informacji nt. skonfigurowanych uprawnień użytkowników systemu (art.5 ust. 1, lit. f, art. 5 ust. 2) |  | *Proszę o wskazanie, czy z systemu możliwe jest wygenerowanie raportu zawierającego informacje o zarejestrowanych/ wyrejestrowanych/ zablokowanych użytkownikach wraz z datami rejestracji/ wyrejestrowania/ zablokowania* |
|  | System zapewnia funkcjonalność anonimizacji lub pseudonimizacji danych osobowych (art. 32 ust. 1, lit. a) |  |  |
|  | System zapewnia funkcjonalność sprostowania (aktualizacji) danych (art.5 ust. 1, lit. d) |  | *Proszę o wskazanie, czy system zapewnia możliwość sprostowania (skorygowania) danych z odnotowaniem informacji na powyższy temat. Uwaga, system nie powinien „pamiętać’ błędnej danej, z wyjątkiem sytuacji, kiedy nastąpiła zmiana danych a odnotowanie faktu tej zmiany wraz z daną poprzednią konieczne jest do identyfikacji osoby, której dane dotyczą (np. zmiana nazwiska)* |
|  | System zapewnia funkcjonalność ograniczenia zakresu przetwarzania danych (np. na uzasadniony wniosek osoby, której dane dotyczą o nadmiarowym charakterze danych) (art. 18) |  |  |
|  | System umożliwia trwałe usuwanie danych, dla których cel przetwarzania został osiągnięty (art. 5, ust. 1, lit. e) |  | *Czy system posiada funkcjonalność raportowania nt. danych osoby, dla której cel przetwarzania został osiągnięty po zadaniu określonego parametru (np. czasu przetwarzania) – przykład: system przetwarza dane kontrahenta, dla którego osiągnięto cel przetwarzania (zrealizowano i rozliczono umowę oraz upłynął ostateczny termin przechowywania danych wynikający z przepisów np. podatkowych – tego typu dane podlegają trwałemu usunięciu)* |
|  | System umożliwia trwałe usuwanie danych na wniosek osoby, której dane dotyczą (art. 17) |  |  |
|  | System umożliwia trwałe usuwanie pojedynczych rekordów zawierających dane osobowe z archiwów i kopii zapasowych oraz upublicznionych (art. 5, ust. 1, lit. e, art. 17) |  |  |
|  | System umożliwia oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania (art. 18) |  |  |
|  | System umożliwia odnotowanie sprzeciwu wobec przetwarzania danych osobowych, określonego w art. 21 |  |  |
|  | System umożliwia odnotowanie informacji o źródle danych, w przypadku zbierania danych nie od osoby, której dane dotyczą (art. 15, ust. 1, lit. g) |  |  |
|  | System umożliwia odnotowanie informacji o odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną ujawnione oraz dacie i zakresie tego udostępnienia (art. 15, ust. 1, lit. c) |  |  |
|  | System umożliwia sporządzenie i wydrukowanie raportu dla każdej osoby, której dane osobowe są przetwarzane, zawierającego zakres przetwarzanych danych (art. 15, ust. 3) |  |  |
|  | Czy system posiada funkcjonalność automatycznego profilowania? (art. 21, art. 22) |  |  |
|  | Czy system lub wchodzące w jego skład urządzenia zlokalizowane są poza Europejskim Obszarem Gospodarczym (EOG)? Czy dane przetwarzane w ramach systemu są lub mogą być przetwarzane (w tym przechowywane) poza EOG (bez względu na ich postać, np. w formie zaszyfrowanej)? Czy zdalny dostęp do systemu posiadają osoby świadczące wsparcie (łączące się zdalnie) spoza EOG? |  |  |
|  | System umożliwia odnotowanie zgody m.in. na profilowanie (art. 22) |  |  |
|  | System zapewnia kontrolę jakości danych osobowych (np. kontrola wprowadzanych danych), system posiada zabezpieczenia przed dublowaniem danych (art. 32) |  | *System powinien zapewnić kontrolę jakości wprowadzanych danych tam gdzie to jest możliwe (np. przy wprowadzaniu nr PESEL). System powinien być zabezpieczony przed możliwością podwójnego wprowadzenia danych tej samej osoby (np. poprzez weryfikację jednoznacznie przypisanego danej osobie numeru - PESEL, nr ewidencyjnego/ kadrowego itp.)* |
|  | System posiada funkcjonalność przetwarzania danych wyłącznie w zakresie, niezbędnym do osiągniecia każdego konkretnego celu przetwarzania (art. 25 ust. 2). |  | *Funkcjonalność, o której mowa w niniejszym punkcie polega na stosowaniu mechanizmów zabezpieczających przed zbyt małą lub zbyt duża ilością pól do wypełnienia (np. stosowanie i weryfikacja przez system wypełniania pól obowiązkowych). Celem ustawodawcy jest ograniczenie nadmiarowości przetwarzania danych osobowych (to jedno z głównych założeń RODO) – w tym celu np. ogranicza się możliwą do wypełnienia ilość pól w systemie (jest ich tylko tyle ile powinno), możliwy jest również mechanizm wykluczający nadmiarowe dane – jeżeli np. pole z nr PESEL jest wypełnione, system blokuje możliwość wypełnienia pola nadmiarowego w postaci nr dokumentu tożsamości.* |
|  | System zapewnia zdolność szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w przypadku wystąpienia incydentu fizycznego lub technicznego (art. 32 ust. 1) |  | *System powinien posiadać funkcjonalność szybkiego przywrócenia jego funkcjonowania i dostępności danych np. poprzez zapewnienie odpowiednich narzędzi informatycznych zarówno do tworzenia backupu jak i szybkiego ich przywrócenia (backup zarówno danych jak i systemu – patrz kolejny punkt). Kwestia wystąpienia incydentu fizycznego i technicznego to stała dostępność np. części zamiennych* |
|  | Dane osobowe przetwarzane w systemie zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych (art. 32) |  | *Pytanie wiąże się z pytaniem z poz. 23 – system musi zapewnić funkcjonalność tworzenia kopii zapasowych (zarówno danych jak i systemu) – funkcjonalność po stronie dostawcy, administrator odpowiedzialny jest za realizację tego procesu* |
|  | Dane przetwarzane w systemie zabezpieczone są przed działalnością szkodliwego oprogramowania (powodującego utratę poufności, dostępności i integralności danych) – art. 32 |  | *Czy dane przetwarzane w systemie zabezpieczone są poprzez stosowanie zabezpieczeń informatycznych (np. system antywirusowy, firewall itp.)?* |
|  | System zabezpieczony jest przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (art. 32) |  | *Czy system zabezpieczony jest poprzez stosowanie np. urządzenia podtrzymującego napięcie (UPS) lub redundantnego zasilania* |
|  | System zabezpieczony jest przed dostępem osób nieuprawnionych (art. 32) |  | *Proszę wskazać sposób zabezpieczenia fizycznego sytemu przed dostępem osób nieuprawnionych, np. serwerowni, stosowanie rozwiązań informatycznych np. wdrożone polityki bezpieczeństwa, w tym polityka haseł, stosowanie ról w systemie o różnym poziomie dostępu, szyfrowana transmisja danych pomiędzy klientem a serwerem itp.* |
|  | Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem (art. 32) |  |  |
|  | Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności (art. 32, art.5 ust.1 lit. e) |  |  |
|  | System umożliwia tworzenie notyfikacji dotyczących naruszeń i incydentów (jeżeli nie, to jak realizowane są te działania – proszę określić w komentarzu – art. 32) |  |  |
|  | System zapewnia funkcjonalność umożliwiającą eksport danych osobowych do powszechnie używanego, ustrukturyzowanego formatu nadającego się do odczytu maszynowego (proszę określić, jaki to format – art. 20) |  |  |
|  | Czy w systemie przeprowadzane jest regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania danych (art. 32, ust. 1) |  | *Proszę o wskazanie sposobów dokonywania przeglądów systemu i nośników danych oraz odnotowywania tego faktu (prowadzenie dziennika, rejestru itp.), zarządzania nośnikami danych, testowania nowych funkcjonalności/ poprawek itp. (np. serwer testowy)* |
|  | W systemie instalowane są na bieżąco poprawki/ aktualizacje producenta, mające na celu zabezpieczenie danych przed utratą poufności, integralności i dostępności (art. 32) |  |  |

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). [↑](#footnote-ref-1)