Załącznik nr 3

do Umowy powierzenia przetwarzania danych osobowych

**Ankieta dla Podmiotu Przetwarzającego**   
weryfikująca wdrożone środki techniczne i organizacyjne  
w zakresie spełniania minimalnych wymagań gwarantujących przetwarzanie danych osobowych  
w sposób zgodny z wymaganiami RODO[[1]](#footnote-1)

| **L.p** | **Element zabezpieczenia**  **{komentarz}** | **Do wypełnienia przez Podmiot Przetwarzający** | |
| --- | --- | --- | --- |
| **Opis zastosowania elementu zabezpieczenia** **{oczekiwana konwencja wpisu:  TAK/NIE: opis odnoszący się do pytania[[2]](#footnote-2)}** | **Komentarz/uzasadnienie odstąpienia od elementu zabezpieczenia** |
|  | Czy Podmiot wyznaczył i poprawnie zgłosił IOD[[3]](#footnote-3) do organu nadzorczego[[4]](#footnote-4)? {jeśli tak: proszę podać kontakt do IOD} |  |  |
|  | Jakie formalne kompetencje posiada IOD do pełnienia swej funkcji?  {proszę podać kierunkowe kursy, szkole­nia, w tym organizowane przez Podmiot przetwarzający – wraz z datami uczestnic­twa} |  |  |
|  | W jaki sposób Podmiot zapewnił IOD:   1. bezzwłoczne włączanie do spraw związanych z przetwarzaniem da­nych osobowych 2. niezależność i wsparcie w działa­niach   {proszę podać konkretne zapisy z poli­tyk/procedur/pełnomocnictw/decyzji itp.} |  |  |
|  | Czy podmiot wyznaczył osobę zastępu­jącą IOD/zespół wspierający pracę IOD? {proszę opisać sposób realizacji zadania} |  |  |
|  | Czy Podmiot opracował, wdrożył i stosuje Politykę Bezpieczeństwa oraz procedury, instrukcje, rejestry normujące zasady przetwarzania danych osobo­wych?  {proszę wskazać z nazwy wdrożone dokumenty wraz z krótkim opisem normowanego przez nie zakresu.} |  |  |
|  | Czy Podmiot wdrożył powszechnie uznane rozwiązania zabezpieczenia? {proszę wskazać wdrożone rozwiązania, w tym np.: normy ISO z grup: ISO 27000, 29000 i 31000; Stosowane zatwierdzo­ne kodeksy postępowania, o których mowa w art. 40 RODO (jeżeli dotyczy), lub zatwierdzone me­chanizmy certyfikacji, o którym mowa wart. 42 RODO} |  |  |
|  | Czy Podmiot wdrożył i testuje mechanizmy obsługi incydentów?  {proszę o odpowiedź: tak/nie/w trakcie[[5]](#footnote-5)} |  |  |
|  | Czy Podmiot wdrożył i testuje plany ciągłości działania?  {proszę o odpowiedź: tak/nie/w trakcie[[6]](#footnote-6)} |  |  |
|  | Czy podmiot będzie przetwarzał powie­rzone dane w systemach informatycz­nych?  {Jeżeli tak, proszę wskazać dla każdego  z systemów (oprócz identyfikującej system na­zwy):   1. zakres przetwarzanych danych; 2. lokację fizyczną i logiczną systemu  i danych; 3. przepływy danych między kompo­nentami systemu z uwzględnieniem puli/zakresu przesyłanych danych; 4. sposób zabezpieczenia dla każdego z komponentów systemu (np. szy­frowanie, pseudonimizacja, uwie­rzytelnianie dostępu, zasady doty­czące tworzenia i zarzą­dzania ko­piami bezpieczeństwa, monitoro­wanie/logi z działań; 5. czy stosuje się walida­cję / weryfika­cję integralności / autentyczności da­nych; 6. ogólny opis sposobu separacji danych Administratora od innych danych w systemie (danych innych Administratorów); 7. ogólny opis sposobu usuwania /aktualizacji danych na wniosek Administratora[[7]](#footnote-7); 8. czy stosuje się rozdział środowiska testowego od produkcyjnego; 9. sposób serwisowania z uwzględnie­niem dostępu firm serwisujących i ich dostępu do danych; 10. grupy funkcyjne osób mających dostęp do systemu / zasady przydzielania dostępu; 11. inne istotne zastosowane środki za­bezpieczenia technicznego, fizycz­nego i organizacyjnego.}   {zaleca się możliwie syntetyczny opis,  a w zakresie prezentacji przepływów zalecaną formą jest diagram.  W systemach informatycznych należy uwzględnić również zabezpieczenia poczty elektronicznej[[8]](#footnote-8).} |  |  |
|  | W przypadku zgody Administratora  i chęci Podmiotu na podpowierzenie przetwarzania danych:   * W jakim zakresie Podmiot chce podpowierzyć przetwarzanie tych danych? * W jaki sposób u podwykonawcy nadzorowany jest proces ochrony  i zabezpieczenia danych? * Czy w ramach podpowierzenia dane opuszczą EOG, a jeśli tak, to do jakiego kraju trafią dane oraz jakie będą stosowane mechanizmy zabezpieczenia? |  |  |
|  | Czy Podmiot prowadzi okresowe audyty zgodności przetwarzania danych osobowych z wymaganiami RODO?  {Jeżeli tak, proszę wskazać stosowaną(e) metodę(y), w tym standardy} |  |  |
|  | Czy Podmiot prowadził szacowanie ryzyka /ocenę skutków przetwarzania dla zadań, które przyjmuje do realizacji  w ramach powierzenia przetwarzania we własnym środowisku?  {Jeżeli tak, proszę wskazać wyniki tych działań, w tym informację o zidentyfikowanych ryzykach} |  |  |
|  | Czy w przeszłości były przeprowadzone kontrole przez organ(y) nadzorczy(e)?  Jeśli tak, to jaka była tego przyczyna?  {proszę o odpowiedź: tak/nie, wraz  z ewentualnym, krótkim opisem przyczyny} |  |  |
|  | W jaki sposób osoby mające dostęp do danych osobowych zostały zapoznane  z przepisami dotyczącymi ochrony danych osobowych i zobowiązane do ich przestrzegania? |  |  |
|  | Czy osoby mające dostęp do danych osobowych zostały zobowiązane do zachowania przetwarzanych danych  w tajemnicy (w tym również po ustaniu zatrudnienia/współpracy)? |  |  |
|  | Jakie są zasady nadawania i dokumento­wania dostępu do:   * przetwarzania danych osobowych? * systemów informatycznych? |  |  |
|  | Jakie zasady regulują dostęp do stref  i pomieszczeń w których przetwarzane będą powierzone Podmiotowi dane przez Administratora?  Jakie techniczne rozwiązania są stosowane do kontroli ruchu osobowego i materiałowego (w zakresie zasobów zawierających ww. dane)?  {Należy rozróżnić pomieszczenia zwykłe od specjalnych typu serwerownia oraz uwzględnić poszczególne fizyczne lokacje własne i w podmiotach świadczących usługi podpowierzenia} |  |  |
|  | W jaki sposób przesyłane są nośniki za­wierające dane osobowe?  {Dotyczy zarówno przesyłanych nośni­ków informatycznych jak też dokumen­tów w formie papierowej. Proszę o uwzględnienie -jeżeli zastosowano w działaniu- różnic między operatorem a operatorem wyznaczonym} |  |  |
|  | Czy Podmiot przetwarza dane wielu Administratorów? {Jeśli tak, to jakie mechanizmy zostały wdrożone by zabezpieczyć te procesy?} |  |  |

……………………………………………………………………………………….…..

podpis i pieczęć osoby reprezentującej Przetwarzającego

1. Rozporządzenie 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)
2. W wymaganych przypadkach w formie załącznika do niniejszej ankiety. [↑](#footnote-ref-2)
3. Inspektor Ochrony Danych – vide art. 37-29 RODO. Poprawne zgłoszenie – vide: Rozdział 2 ustawy z 10 maja 2018 o ochronie danych osobowych. [↑](#footnote-ref-3)
4. Vide art. 4 pkt 21 RODO. [↑](#footnote-ref-4)
5. Wymagany krótki komentarz, jeżeli wdrożone rozwiązanie nie jest kompletne. [↑](#footnote-ref-5)
6. Wymagany krótki komentarz, jeżeli wdrożone rozwiązanie nie jest kompletne. [↑](#footnote-ref-6)
7. Chodzi o retencję danych. [↑](#footnote-ref-7)
8. W tym np. sposobu uzgadniania metod szyfrowania i przekazania haseł. [↑](#footnote-ref-8)