**Załącznik nr 2 do Regulaminu**

**określającego wymagania dotyczące ochrony danych osobowych  
i bezpieczeństwa informacji w zamówieniach publicznych**

**Oświadczenie dotyczące ochrony danych osobowych**

W związku z postępowaniem o udzielenie zamówienia wyłączonego spod regulacji ustawy Prawo zamówień publicznych, przed udzieleniem zamówienia, wykonawca zobowiązany jest do podpisania oświadczenia w zakresie zdolności wykonawcy do wykonania zamówienia, zgodnie z obowiązującymi zasadami ochrony danych osobowych i elementami bezpieczeństwa informacji.

Nazwa i adres wykonawcy:

..............................................................................................................................................................................................................................................................................................................

1. Oświadczam, że wykonawca wskazany powyżej:
2. spełnia wymagania określone w RODO[[1]](#footnote-1), a w szczególności wskazane w art. 28, 29, 30, 32, 33;
3. gwarantuje, że dostęp do powierzonych w związku z realizacją zamówienia danych osobowych będą miały wyłącznie osoby upoważnione, a wykonawca posiada w tym zakresie odpowiednie procedury i jest w stanie wykazać ich stosowanie;
4. wyznaczy do realizacji zamówienia pracowników/współpracowników przeszkolonych w zakresie ochrony danych osobowych;
5. gwarantuje, że pomieszczenia, w których będą przetwarzane powierzone w związku z realizacją zamówienia dane osobowe będą odpowiednio zabezpieczone (w szczególności samodzielny dostęp do nich będą miały wyłącznie osoby upoważnione do przetwarzania tych danych) oraz, że posiada w tym zakresie odpowiednie procedury i jest w stanie wykazać ich stosowanie.

……………………………………………………..

Podpis wykonawcy

1. Oświadczam, że wykonawca wskazany powyżej [[2]](#footnote-2):
2. zobowiązuje się do stosowania adekwatnych do zagrożeń środków ochrony przetwarzanych informacji (w tym danych osobowych) przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, obejmujących, m.in., poniżej wskazane zabezpieczenia techniczno-organizacyjne:
3. zapewnienie aktualizacji regulacji wewnętrznych z obszaru bezpieczeństwa informacji adekwatnie do zagrożeń,
4. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
5. podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji,
6. bezzwłoczną zmianę uprawnień, w przypadku zmiany zadań osób, o których mowa w punkcie poprzedzającym,
7. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień, jak:

* zagrożenia bezpieczeństwa informacji,
* skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
* stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich,

1. zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

* monitorowanie dostępu do informacji,
* czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
* stosowanie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,

1. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
2. zabezpieczenie informacji w sposób uniemożliwiający nieuprawnione jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
3. zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
4. zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

* dbałości o aktualizację oprogramowania,
* minimalizowaniu ryzyka utraty informacji w wyniku awarii,
* ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
* stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
* zapewnieniu bezpieczeństwa plików systemowych,
* redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
* niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
* kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa,

1. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
2. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji i testów penetracyjnych.
3. wyraża zgodę na przeprowadzanie przez zamawiającego testów bezpieczeństwa oferowanych rozwiązań teleinformatycznych, po uprzednim uzgodnieniu przez strony szczegółów z tym związanych, oraz zobowiązuje się uzyskać wymagane zgody od podwykonawców, o ile będzie miało to zastosowanie.

…………………………………………………

Podpis wykonawcy

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. Dotyczy wykonawcy, który dostarczy lub udostępni zamawiającemu rozwiązanie informatyczne wykorzystywane do przetwarzania danych zamawiającego (usługa przetwarzania danych, systemy, oprogramowanie, aplikacje). [↑](#footnote-ref-2)