**Załącznik nr 1 do Regulaminu**

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

**Wymagania ochrony danych osobowych i bezpieczeństwa informacji**

1. W celu wykazania zdolności do wykonania zamówienia, zgodnie z obowiązującymi zasadami ochrony danych osobowych i elementami bezpieczeństwa informacji, wykonawca zobowiązany jest do:
2. spełnienia wymagań określonych w RODO, a w szczególności wskazanych w art. 28, 29, 30, 32, 33;
3. zagwarantowania dostępu do powierzonych w związku z realizacją zamówienia danych osobowych wyłącznie osobom upoważnionym oraz posiadania w tym zakresie odpowiednich procedur i możliwości wykazania ich stosowania;
4. wyznaczenia do realizacji zamówienia pracowników/współpracowników przeszkolonych w zakresie ochrony danych osobowych;
5. zagwarantowania, 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), posiadania w tym zakresie odpowiednich procedur oraz możliwości wykazania ich stosowania.
6. Jeżeli wykonawca dostarczy lub udostępni zamawiającemu rozwiązanie informatyczne wykorzystywane do przetwarzania danych zamawiającego (usługa przetwarzania danych, oprogramowanie, systemy, aplikacje), zobowiązany jest 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:
7. zapewnienie aktualizacji regulacji wewnętrznych z obszaru bezpieczeństwa informacji adekwatnie do zagrożeń;
8. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
9. 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;
10. bezzwłoczną zmianę uprawnień, w przypadku zmiany zadań osób, o których mowa w punkcie poprzedzającym;
11. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień, jak:
    1. zagrożenia bezpieczeństwa informacji,
    2. skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
    3. stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich;
12. zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
    1. monitorowanie dostępu do informacji,
    2. czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
    3. stosowanie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
13. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
14. zabezpieczenie informacji w sposób uniemożliwiający nieuprawnione jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
15. zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
16. zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
    1. dbałości o aktualizację oprogramowania,
    2. minimalizowaniu ryzyka utraty informacji w wyniku awarii,
    3. ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
    4. stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
    5. zapewnieniu bezpieczeństwa plików systemowych,
    6. redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
    7. niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
    8. kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
17. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
18. zapewnienia okresowego audytu i testów penetracyjnych w zakresie bezpieczeństwa informacji.