

Warszawa, dnia 25.05.2023 r.

MODYFIKACJA I WYJAŚNIENIA DO ZAPYTANIA OFERTOWEGO**Znak sprawy: 38/DK/2023****Przedmiot zamówienia publicznego:**

„Zakup oraz dostarczenie do siedziby Zamawiającego bonów towarowych/kuponów podarunkowych/kart podarunkowych różnego przeznaczenia na sprzęt RTV/AGD na potrzeby Europejskiego Konkursu Statystycznego (Statistical Literacy Project) w ramach umowy o dotację nr 101096593-2022-PL-COMPETITION, Nazwa projektu: Udział w Europejskim Konkursie Statystycznym 2022/2023”.

Pytanie 1:

Proszę o udostępnienie draftu umowy, o której jest informacja w zapytaniu ofertowym.

Odpowiedź Zamawiającego:

Zamawiający w załączeniu przedstawia główne założenia do Umowy.

Pytanie 2:

Proszę również o informację czy na dokumencie musi podpisać się osoba posiadająca Pełnomocnictwo do reprezentowania spółki?

Czy oferta może zostać wysłana w postaci PDF-a pod podpisu kwalifikowanego ale w postaci skanu?

Odpowiedź Zamawiającego:

Zgodnie z pkt V ppkt 2 zapytania ofertowego „Oferta i/lub oświadczenia muszą być podpisane przez osobę/osoby uprawnione do reprezentowania i składania oświadczeń woli w imieniu Wykonawcy”.

Przez osobę upoważnioną do występowania i podpisywania w imieniu Wykonawcy, należy rozumieć osobę wymienioną w dokumencie uprawniającym Wykonawcę do występowania w obrocie prawnym.

W przypadku gdy upoważnienie do podpisania oferty/oświadczeń nie wynika bezpośrednio z właściwego rejestru, niezbędne jest dołączenie do oferty pełnomocnictwa wystawionego przez osoby do tego upoważnione. (Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez upoważnionego).

Treść pełnomocnictwa musi jednoznacznie określać czynności, co do wykonywania których pełnomocnik jest upoważniony. W przypadku gdyby pełnomocnictwa udzielała osoba inna niż uprawniona z mocy prawa lub umowy spółki do reprezentowania podmiotu, do oferty należy dołączyć również pełnomocnictwo do dokonania tej czynności.

Wypełnioną i podpisaną ofertę należy złożyć w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym przez osobę uprawnioną do występowania w imieniu Wykonawcy lub jako elektroniczne odwzorowanie (skan) dokumentu posiadającego postać papierową i podpisanego własnoręcznie przez osobę uprawnioną do występowania w imieniu Wykonawcy lub uwierzytelnioną za pomocą profilu zaufanego, za pośrednictwem poczty elektronicznej wskazany w pkt V ppkt. 12 Zapytania ofertowego

Pytanie 3:

W podanym zapytaniu pojawią się takie zdanie:

„Bony towarowe/kupony podarunkowe/karty podarunkowe powinny umożliwiać zakup w sklepach ze sprzętem RTV/AGD. Zamawiający nie dopuszcza bonów, które są możliwe do realizacji w jednej sieci sklepów.”

Proszę doprecyzować. (...).

Odpowiedź Zamawiającego:

Zamawiający dokonał modyfikacji zapisów Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do Zapytania ofertowego. W aktualnym brzmieniu pkt I otrzymuje brzmienie: Bony towarowe/kupony podarunkowe/karty podarunkowe powinny umożliwiać zakup w sklepach ze sprzętem RTV/AGD. Zamawiający wymaga zapewnienia realizacji bonów w minimalnie 300 punktach sklepowych na terenie całego kraju.

Zamawiający dokonał następujących modyfikacji zapytania ofertowego:

Zapytanie ofertowe – pkt II. 1) - było**1. Sposób wykonania zamówienia publicznego oraz wymagania dotyczące realizacji przedmiotu:**

Przedmiot zamówienia obejmuje dostawę bonów towarowych różnego przeznaczenia do realizacji w punktach sprzedaży na terenie całego kraju **na zakup sprzętu RTV/AGD o terminie ważności minimum 12 miesięcy od daty podpisania protokołu odbioru z wynikiem pozytywnym.**

Bony towarowe o następujących nominałach:

Nominał	Liczba sztuk	Ogólna wartość
Europejski Konkurs Statystyczny		
50 zł	100	5 000 zł
100 zł	270	27 000 zł
ŁĄCZNIE		
	370	32 000 zł

Bony towarowe/kupony podarunkowe/karty podarunkowe powinny umożliwiać zakup w sklepach ze sprzętem RTV/AGD. Zamawiający nie dopuszcza bonów, które są możliwe do realizacji w jednej sieci sklepów. Szczegółowy zakres i sposób realizacji przedmiotu zamówienia określa „Opis przedmiotu zamówienia”, stanowiący Załącznik nr 1 do Zapytania ofertowego.

Zapytanie ofertowe – pkt II. 1) – powinno być**1. Sposób wykonania zamówienia publicznego oraz wymagania dotyczące realizacji przedmiotu:**

Przedmiot zamówienia obejmuje dostawę bonów towarowych różnego przeznaczenia do realizacji w punktach sprzedaży na terenie całego kraju **na zakup sprzętu RTV/AGD o terminie ważności minimum 12 miesięcy od daty podpisania protokołu odbioru z wynikiem pozytywnym.**

Bony towarowe o następujących nominałach:

Nominał	Liczba sztuk	Ogólna wartość
Europejski Konkurs Statystyczny		
50 zł	100	5 000 zł
100 zł	270	27 000 zł
ŁĄCZNIE		
	370	32 000 zł

Bony towarowe/kupony podarunkowe/karty podarunkowe powinny umożliwiać zakup w sklepach ze sprzętem RTV/AGD. Zamawiający wymaga zapewnienia realizacji bonów w minimalnie 300 punktach sklepowych na terenie całego kraju.

Szczegółowy zakres i sposób realizacji przedmiotu zamówienia określa „Opis przedmiotu zamówienia”, stanowiący Załącznik nr 1 do Zapytania ofertowego.

Z poważaniem
Karolina Banaszek
Z-ca Dyrektora Departamentu
Edukacji i Komunikacji



Signed by /
Podpisano przez:

Karolina Barbara
Banaszek
Główny Urząd
Statystyczny

Date / Data:
2023-05-25 12:39

Załączniki:

1. Opis przedmiotu zamówienia - zmieniony w dniu 25-05-2023 r.;
2. Formularz oferty (wzór) - zmieniony w dniu 25-05-2023 r.

Główne założenia do Umowy nr 38/DK/2023

Zawarta w dniu 2023 roku pomiędzy: Skarbem Państwa – Głównym Urzędem Statystycznym z siedzibą w (00-925) Warszawie przy al. Niepodległości 208, posiadającym NIP: 526-10-40-828 oraz REGON: 000331501, zwanym dalej „Zamawiającym”, reprezentowanym przez:

.....
a

..... z siedzibą w przy ul., kod, wpisaną do rejestru przedsiębiorców (w przypadku przedsiębiorcy wpisanego do KRS), przez Sąd Rejonowy Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: (NIP, REGON, zwaną dalej „Wykonawcą”, reprezentowaną przez:

.....
łącznie zwanymi „Stronami”, została zawarta umowa następującej treści, zwana dalej „Umową”:

§ 1. Przedmiot Umowy

1. Przedmiotem Umowy jest Zakup oraz dostarczenie do siedziby Zamawiającego bonów towarowych/kuponów podarunkowych/kart podarunkowych różnego przeznaczenia na sprzęt RTV/AGD na potrzeby Europejskiego Konkursu Statystycznego (Statistical Literacy Project) w ramach umowy o dotację nr 101096593-2022-PL-COMPETITION, Nazwa projektu: Udział w Europejskim Konkursie Statystycznym 2022/2023, o podanych niżej nominałach i w następujących ilościach:
 - 1) 50,00 zł (słownie: pięćdziesiąt złotych 00/100) - 100 (słownie: sto) sztuk,
 - 2) 100,00 zł (słownie: sto złotych 00/100) - 270 (słownie: dwieście siedemdziesiąt) sztuk,zwanymi dalej „Bonami”.
2. Bony będą oznakowane w sposób umożliwiający zakup asortymentu z grupy RTV-AGD.
3. Termin ważności Bonów wynosi (zgodnie z deklaracją Wykonawcy) miesiące/y, licząc od daty podpisanego z wynikiem pozytywnym Protokołu odbioru, którego wzór stanowi Załącznik nr 1 do Umowy.

§ 2. Obowiązki Wykonawcy

1. Wykonawca zobowiązuje się dostarczyć przedmiot umowy zgodnie z wymaganiami i w ilościach określonych przez Zamawiającego.
2. Bony zostaną dostarczone jednorazowo, na koszt i ryzyko Wykonawcy.
3. Wykonawca dostarczy przedmiot umowy do siedziby GUS w miejsce wskazane przez Zamawiającego, po uprzednim ustaleniu z Zamawiającym dnia, w którym odbędzie się dostawa.
4. W ramach spełnienia klauzuli środowiskowej dostarczenie przedmiotu umowy odbędzie się poza godzinami szczytu komunikacyjnego, tj. w godz. 9.00-14.00. W przypadku dostawy w godzinach innych niż wskazane, Zamawiający naliczy karę, o której mowa w § 6 ust. 1 pkt 5.
5. Fakt dostarczenia i odbioru, jak również stan jakościowy i ilościowy przedmiotu umowy, zostanie potwierdzony w Protokole odbioru, którego wzór stanowi Załącznik nr 1 do Umowy, sporządzonym przez Zamawiającego i podpisanym przez uprawnionych przedstawicieli Stron.
6. Podpisany z wynikiem pozytywnym Protokół odbioru będzie stanowił podstawę do wystawienia przez Wykonawcę noty obciążeniowej oraz jej zapłaty przez Zamawiającego.
7. W przypadku uszkodzenia/usterki technicznej bonu w okresie ważności Wykonawca gwarantuje jego wymianę w ciągu 3 dni roboczych od dnia zgłoszenia.
8. Zamawiający bez jakichkolwiek roszczeń finansowych ze strony Wykonawcy, może odmówić przyjęcia dostawy w całości, jeżeli przedmiot Umowy:
 - 1) nie będzie wolny od wad fizycznych;
 - 2) nie zostanie dostarczony zgodnie z wymaganiami Zamawiającego.

§ 3. Terminy

1. Wykonawca dostarczy przedmiot Umowy do siedziby Zamawiającego w terminie do 5 dni roboczych od daty podpisania Umowy.
2. Termin realizacji Umowy, o którym mowa w ust. 1, będzie uznany za dotrzymany, gdy w tym terminie zostanie podpisany, z wynikiem pozytywnym, przez przedstawicieli Wykonawcy i Zamawiającego Protokół odbioru przedmiotu Umowy.

§ 4. Koordynatorzy Umowy

1. Osobą wskazaną do współpracy ze strony Wykonawcy oraz odpowiedzialną za realizację Umowy jest:
....., tel., e-mail:
2. Osobami uprawnionymi do uzgadniania na bieżąco spraw związanych z realizacją przedmiotu Umowy, w tym do odbioru przedmiotu Umowy i podpisania Protokołu odbioru przedmiotu Umowy ze strony Zamawiającego są:
 - 1) – tel., e-mail:
 - 2) – tel., e-mail:
3. Osobami wskazanymi do współpracy ze strony Zamawiającego w zakresie kontroli postanowień realizacji klauzuli środowiskowej, o której mowa w § 2 ust. 4, są:
 - 1) – tel., e-mail:.....;
 - 2) – tel., e-mail:.....;
 - 3) – tel., e-mail:
4. Zmiana osób wskazanych w ust. 1-3 dla zachowania skuteczności wymaga uprzedniego poinformowania drugiej strony, z co najmniej dwudniowym wyprzedzeniem, za pośrednictwem poczty elektronicznej.

§ 5. Wartość Umowy

1. Za wykonanie przedmiotu Umowy, o którym mowa w § 1, Wykonawca otrzyma wynagrodzenie, określone na podstawie Oferty zawierającej Formularz cenowy, która stanowi Załącznik nr 2 do Umowy, w łącznej wysokości: zł (słownie:..... zł 00/100), odpowiadającej łącznej nominalnej wartości faktycznie zamówionych i dostarczonych Bonów.
2. Podstawą do zapłaty wynagrodzenia będzie prawidłowo wystawiona i dostarczona przez Wykonawcę nota obciążeniowa, do której Wykonawca zobowiązany jest załączyć oryginał podpisanego z wynikiem pozytywnym Protokołu odbioru przedmiotu Umowy.
3. Wykonawca zobowiązuje się dostarczyć prawidłowo wystawioną notę obciążeniową w terminie do 5 dni od daty podpisania Protokołu odbioru przedmiotu Umowy z wynikiem pozytywnym.
4. Zamawiający dokona zapłaty wynagrodzenia przelewem, na rachunek bankowy Wykonawcy wskazany na nocie obciążeniowej, w terminie do 14 dni od daty dostarczenia do Zamawiającego prawidłowo wystawionej noty obciążeniowej.
5. Wynagrodzenie będzie płatne ze środków umowy o dotację pt. „Udział w Europejskim Konkursie Statystycznym 2022/2023 nr 101096593-2022-PL-COMPETITION”.
6. Na podstawie ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz. U. z 2020 r. poz. 1666) Zamawiający umożliwia Wykonawcy przesłanie ustrukturyzowanej faktury elektronicznej, faktur korygujących i not księgowych za pośrednictwem platformy elektronicznego fakturowania.
Usługi Platformy Elektronicznego Fakturowania są świadczone pod adresami:
 - 1) <https://efaktura.gov.pl> (Portal PEF),
 - 2) <https://brokerpefexpert.efaktura.gov.pl> (Broker PEFexpert) – obsługujący Zamawiającego,
 - 3) <https://brokerinfinite.efaktura.gov.pl> (Broker Infinite)
7. Zamawiający zastrzega, że nie dopuszcza przesyłania za pośrednictwem platformy elektronicznego fakturowania innych dokumentów wymienionych w rozporządzeniu Ministra Przedsiębiorczości i Technologii z dnia 25 kwietnia 2019 r. w sprawie listy innych ustrukturyzowanych dokumentów elektronicznych, które mogą być przesyłane za pośrednictwem platformy elektronicznego fakturowania służącej do przesyłania ustrukturyzowanych faktur elektronicznych oraz innych ustrukturyzowanych dokumentów elektronicznych (Dz. U. z 2019 r. poz. 856).

8. Za dotrzymanie terminu zapłaty, o którym mowa w ust. 4, uważa się dzień uznania rachunku bankowego Wykonawcy.
9. Wykonawca oświadcza, że numer rachunku rozliczeniowego wskazany w nocie obciążeniowej, która będzie wystawiona w jego imieniu, *jest rachunkiem/nie jest rachunkiem* (zgodnie z oświadczeniem Wykonawcy złożonym w ofercie), dla którego zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - Prawo Bankowe (Dz. U. z 2021 r. poz. 2439, z późn. zm.) prowadzony jest rachunek VAT.
10. Wykonawca oświadcza, że podany numer rachunku rozliczeniowego wskazany w nocie obciążeniowej, *jest taki sam/nie jest taki sam* jak w rejestrze podatników (biała lista).

§ 6. Kary Umowne

1. Wykonawca zapłaci Zamawiającemu kary umowne, które będą naliczane w następujących okolicznościach i wysokościach:
 - 1) w przypadku zwłoki w realizacji przedmiotu Umowy w terminie, o którym mowa w § 3 ust. 1, w wysokości 0,5% wynagrodzenia brutto, o którym mowa w § 5 ust. 1, za każdy rozpoczęty dzień zwłoki, nie więcej niż 10% tego wynagrodzenia,
 - 2) za każde udokumentowane naruszenie zasad zachowania poufności Informacji Poufnych, o których mowa w § 8, w wysokości 1000 zł (słownie: jeden tysiąc zł 00/100);
 - 3) za każde udokumentowane naruszenie wymagań bezpieczeństwa informacji, o których mowa w § 10, w wysokości 10% wynagrodzenia brutto określonego w § 5 ust. 1,
 - 4) za każdy stwierdzony brak spełnienia obowiązku, o którym mowa w § 12 ust. 3, w wysokości 10% wynagrodzenia brutto określonego w § 5 ust. 1,
 - 5) w przypadku niespełnienia klauzuli środowiskowej, o której mowa w § 2 ust. 4, w wysokości 500 zł brutto (słownie: pięćset zł 00/100),
 - 6) za odstąpienie Wykonawcy od Umowy lub rozwiązanie Umowy przez Wykonawcę z przyczyn leżących po jego stronie, w wysokości 20% wynagrodzenia brutto, o którym mowa w § 5 ust. 1,
 - 7) za odstąpienie Zamawiającego od Umowy lub rozwiązanie Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, w wysokości 20% wynagrodzenia brutto, o którym mowa w § 5 ust. 1.
2. Kary umowne, o których mowa w ust. 1 pkt 1 - 5 podlegają sumowaniu.
3. Łączna maksymalna wysokość naliczonych kar umownych nie może przekroczyć 20 % wartości brutto Umowy określonej w § 5 ust. 1
4. Na podstawie przepisów ogólnych Kodeksu cywilnego Zamawiający zastrzega sobie prawo do odszkodowania uzupełniającego, przewyższającego wysokość kar umownych, do wysokości rzeczywiście poniesionej szkody.
5. Wykonawca wyraża zgodę na potrącenie kar umownych z przysługującego mu wynagrodzenia lub zapłatę kary na podstawie księgowej noty obciążeniowej.

§ 7. Siła Wyższa

1. Termin „Siła wyższa” oznacza zewnętrzne, niemożliwe do przewidzenia i zapobieżenia zdarzenie występujące po zawarciu Umowy, uniemożliwiające należyte wykonanie przez Stronę jej obowiązków, w szczególności takie jak katastrofy naturalne, wojny, ataki terrorystyczne.
2. Żadna strona nie będzie odpowiedzialna za niewykonanie lub nienależyte wykonanie swoich zobowiązań w ramach Umowy, jeżeli niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy jest wynikiem działania Siły wyższej.
3. Jeżeli zaistnieje Siła wyższa, Strona, której dotyczą okoliczności siły wyższej, bezzwłocznie zawiadomi drugą stronę na piśmie o jej zaistnieniu i przyczynach. Strona, której dotyczą okoliczności Siły wyższej dotoży wszelkich starań, aby niezwłocznie nie dłużej, niż w terminie 2 dni roboczych od daty zawiadomienia przedstawić drugiej stronie dokumentację, która wyjaśnia naturę i przyczyny zaistniałej okoliczności Siły wyższej w takim zakresie, w jakim jest to możliwe. Jeżeli po zawiadomieniu Strony nie uzgodnią inaczej w formie pisemnej, każda ze Stron będzie kontynuowała wysiłki w celu wywiązania się ze swoich zobowiązań.
4. W takim zakresie, w jakim niemożność wykonywania zobowiązań umownych wynika z Siły wyższej oddziałującej na jedną ze Stron, druga strona również nie będzie odpowiedzialna za niewykonanie swoich zobowiązań.

§ 8. Poufność danych i informacji

1. Z zastrzeżeniem postanowienia ust. 2, Wykonawca zobowiązuje się do zachowania poufności wszelkich dotyczących Zamawiającego danych i informacji uzyskanych w jakikolwiek sposób (zamierzony lub przypadkowy) w związku z wykonywaniem Umowy, bez względu na sposób i formę ich przekazania, nazywanych dalej łącznie "Informacjami Poufnymi".
2. Obowiązek, o którym mowa w ust. 1, obowiązuje Wykonawcę przez czas trwania Umowy oraz przez okres 10 lat po jej rozwiązaniu, wygaśnięciu lub odstąpieniu od niej, bez względu na przyczynę.
3. Obowiązku zachowania poufności, o którym mowa w ust. 1, nie stosuje się do danych i informacji:
 - 1) dostępnych publicznie;
 - 2) otrzymanych przez Wykonawcę, zgodnie z przepisami prawa powszechnie obowiązującego, od osoby trzeciej bez obowiązku zachowania poufności;
 - 3) które w momencie ich przekazania przez Zamawiającego były już znane Wykonawcy bez obowiązku zachowania poufności;
 - 4) w stosunku do których Wykonawca uzyskał pisemną zgodę Zamawiającego na ich ujawnienie.
4. W przypadku, gdy ujawnienie Informacji Poufnych przez Wykonawcę jest wymagane na podstawie przepisów prawa powszechnie obowiązującego, Wykonawca poinformuje Zamawiającego o przyczynach i zakresie ujawnionych Informacji Poufnych. Poinformowanie takie powinno nastąpić w formie pisemnej lub w formie wiadomości wysłanej na adres poczty elektronicznej Zamawiającego, chyba że takie poinformowanie Zamawiającego byłoby sprzeczne z przepisami prawa powszechnie obowiązującego.
5. Wykonawca zobowiązuje się do:
 - 1) dołożenia właściwych starań w celu zabezpieczenia Informacji Poufnych przed ich utratą, zniekształceniem oraz dostępem nieupoważnionych osób trzecich;
 - 2) niewykorzystywania Informacji Poufnych w celach innych niż wykonanie Umowy.
6. Wykonawca zobowiązuje się do poinformowania każdej z osób, przy pomocy których wykonuje Umowę i które będą miały dostęp do Informacji Poufnych, o wynikających z Umowy obowiązkach w zakresie zachowania poufności, a także do skutecznego zobowiązania i egzekwowania od tych osób obowiązków w zakresie zachowania poufności. Za ewentualne naruszenia tych obowiązków przez osoby trzecie Wykonawca ponosi odpowiedzialność, jak za własne działania.
7. W przypadku utraty lub zniekształcenia Informacji Poufnych lub dostępu nieupoważnionej osoby trzeciej do Informacji Poufnych, Wykonawca bezzwłocznie podejmie odpowiednie do sytuacji działania ochronne oraz poinformuje o sytuacji Zamawiającego. Poinformowanie takie, w formie pisemnej lub w formie wiadomości wysłanej na adres poczty elektronicznej Zamawiającego, powinno opisywać okoliczności zdarzenia, zakres i skutki utraty, zniekształcenia lub ujawnienia Informacji Poufnych oraz podjęte działania ochronne.
8. Po wykonaniu Umowy oraz w przypadku rozwiązania Umowy lub odstąpienia od Umowy przez którąkolwiek ze Stron, Wykonawca bezzwłocznie zwróci Zamawiającemu lub komisyjnie usunie wszelkie Informacje Poufne w sposób uniemożliwiający ich przywrócenie. W przypadku komisyjnego usunięcia ww. Informacji, Wykonawca jest zobowiązany poinformować Zamawiającego o tym fakcie, bez zbędnej zwłoki.
9. Ustanowione Umową zasady zachowania poufności Informacji Poufnych, jak również przewidziane w Umowie kary umowne z tytułu naruszenia zasad zachowania poufności Informacji Poufnych, obowiązują zarówno podczas wykonania Umowy, jak i po jej wygaśnięciu.
10. W przypadku udokumentowanego naruszenia zasad zachowania poufności Informacji Poufnych, Zamawiający naliczy karę umowną, o której mowa w § 6 ust. 1 pkt 2) Umowy. W sytuacji, o której mowa w zdaniu pierwszym, Zamawiający będzie miał również prawo do odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy i naliczenia kary umownej, o której mowa w § 6 ust. 1 pkt 6) Umowy.

§ 9. Udostępnianie i ochrona danych osobowych

1. Celem realizacji Umowy Strony udostępniają sobie wzajemnie dane osobowe koordynatorów Umowy oraz innych osób realizujących Umowę, w zakresie:
 - a) Wykonawca: imię i nazwisko, numer telefonu oraz adres mailowy pracowników, którzy będą koordynować realizację Umowy ze strony Wykonawcy,
 - b) Zamawiający: imiona i nazwiska, numery telefonów oraz adresy mailowe pracowników, którzy będą koordynować realizację Umowy ze strony Zamawiającego.

2. Z momentem udostępnienia danych Strona otrzymującą dane staje się ich niezależnym administratorem w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (dalej RODO).
3. Każda ze Stron oświadcza, że:
 - 1) jest administratorem danych będących przedmiotem udostępnienia oraz posiada podstawę prawną do ich udostępnienia;
 - 2) będzie przetwarzała udostępnione dane osobowe wyłącznie w celu realizacji Umowy i zgodnie z obowiązującymi przepisami prawa, w tym przepisami RODO;
 - 3) udostępnienie danych zostanie zrealizowane z zachowaniem najwyższych standardów bezpieczeństwa oraz z zapewnieniem przestrzegania zasad określonych w RODO.
4. Wykonawca oświadcza, iż przed zawarciem Umowy zapoznał się z Załącznikiem nr 3 do Umowy (Klauzula informacyjna RODO Zamawiającego) oraz przekazał klauzulę informacyjną Zamawiającego osobom reprezentującym go lub innym osobom realizującym Umowę (obowiązek informacyjny przewidziany w art. 14 RODO). Wykonawca zobowiązuje się, że w przypadku wyznaczenia lub wskazania do działania przy wykonywaniu Umowy dodatkowych osób, najpóźniej wraz z przekazaniem Zamawiającemu danych osobowych tych osób, zrealizować obowiązki informacyjne w trybie art. 14 RODO zawarte w Załączniku nr 3 do Umowy.
5. Wykonawca zobowiązany jest do wypełnienia obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO, wobec Zamawiającego oraz osób, których dane zostały mu udostępnione.

§ 10. Wymagania bezpieczeństwa informacji

1. Wykonawca oświadcza, iż przed zawarciem Umowy zapoznał się z Załącznikiem nr 4 do Umowy (Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych) oraz zobowiązuje się do przestrzegania zawartych w nim wymagań.
2. W przypadku udokumentowanego naruszenia wymagań bezpieczeństwa informacji, Zamawiający naliczy karę umowną, o której mowa w § 6 ust. 1 pkt 3. W sytuacji, o której mowa w zdaniu pierwszym, Zamawiający będzie miał również prawo do odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy i naliczenia kary umownej, o której mowa w § 6 ust. 1 pkt 7).

§ 11. Powierzenie przetwarzania danych osobowych

1. W przypadku powierzenia przetwarzania danych osobowych Wykonawcy, Zamawiający wymaga podpisania przez Wykonawcę umowy powierzenia przetwarzania danych osobowych, której wzór stanowi Załącznik nr 5 do Umowy.
2. W przypadku zmiany zakresu powierzonych danych osobowych, Strony podpiszą aneks do umowy powierzenia, stanowiącej Załącznik nr 5 do Umowy. Zmiana zakresu umowy powierzenia nie stanowi zmiany zapisów niniejszej Umowy.

§ 12. Konflikt interesów

1. Wykonawca oświadcza, że będzie realizował przedmiot Umowy z zachowaniem zasad bezstronności oraz braku konfliktu interesów.
2. Strony przez konflikt interesów rozumieją:
 - 1) pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub związanie z tytułu przysposobienia, opieki lub kurateli z członkami organów zarządzających oraz pracownikami Zamawiającego zaangażowanymi w realizację przedmiotu Umowy;
 - 2) pozostawanie z Zamawiającym w takim stosunku prawnym lub faktycznym, które może budzić uzasadnione wątpliwości co do bezstronności tych osób.
3. Wykonawca w przypadku zaistnienia bądź ujawnienia jakiegokolwiek okoliczności, o której mowa w ust. 2, niezwłocznie powiadomi o tej okoliczności Zamawiającego.
4. Zamawiający może żądać od Wykonawcy zamiany osoby, której dotyczy konflikt interesów, przy czym osoba zastępująca musi posiadać kwalifikacje nie niższe od osoby zastępowanej.
5. W przypadku braku spełnienia obowiązku, o którym mowa w ust. 3, Wykonawca zapłaci Zamawiającemu karę

umowną, w wysokości określonej w § 6 ust 1 pkt 4). W sytuacji, o której mowa w zdaniu pierwszym, Zamawiający będzie miał również prawo do odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy ze skutkiem natychmiastowym i naliczenia kary umownej, o której mowa w § 6 ust. 1 pkt 6).

6. Niewykonanie przez Wykonawcę obowiązku, o którym mowa w ust. 4, równoznaczne jest wykonywaniu świadczenia w sposób sprzeczny z Umową i stanowi przesłankę do odstąpienia przez Zamawiającego od Umowy ze skutkiem natychmiastowym.

§ 13. Odstąpienie od Umowy i rozwiązanie Umowy

1. Zamawiający może odstąpić od Umowy, jeżeli Wykonawca w rażący sposób narusza postanowienia Umowy.
2. Do rażących naruszeń Umowy zalicza się następujące przypadki:
 - 1) kiedy zwłoka Wykonawcy w dochowaniu terminu, o którym mowa w § 3 ust. 1, przekroczy 10 dni;
 - 2) Wykonawca powierzył wykonanie Umowy lub jej części jakiegokolwiek osobie trzeciej bez zgody Zamawiającego wyrażonej w formie pisemnej.
3. W przypadku zaistnienia okoliczności, o której mowa w ust. 2 pkt 2, Zamawiający wezwie pisemnie Wykonawcę do zaniechania naruszeń postanowień Umowy i usunięcia skutków tych naruszeń w terminie 5 dni od dnia doręczenia wezwania. W przypadku bezskutecznego upływu ww. terminu Zamawiającemu przysługuje prawo złożenia oświadczenia o odstąpieniu od Umowy. Termin odstąpienia wynosi 5 dni od upływu terminu określonego w zdaniu pierwszym.
4. Oświadczenie o odstąpieniu od Umowy powinno być sporządzone na piśmie pod rygorem nieważności.
5. Postanowienia ust. 3 nie dotyczą przypadku określonego w ust. 2 pkt 1. W tym przypadku Zamawiającemu przysługuje prawo do wykonania prawa odstąpienia od Umowy bez wyznaczania terminu dodatkowego.
6. W przypadku, o którym mowa w ust. 2 pkt 1, Zamawiający zastrzega sobie prawo do zlecenia wykonania przedmiotu Umowy podmiotowi trzeciemu i obciążenia Wykonawcy kosztami w wysokości różnicy pomiędzy kosztami przewidzianymi w umowie, wynikającymi z realizacji przedmiotu umowy a realnie poniesionymi kosztami. Zamawiający zachowa prawo do naprawienia pełnej szkody.
7. W przypadku wykonania przez Zamawiającego prawa odstąpienia od Umowy, niezależnie od jego podstawy, odstąpienie wywiera skutek wyłącznie co do części niewykonanej. W związku z powyższym żadna ze Stron nie będzie zobowiązana do zwrotu świadczeń otrzymanych od drugiej Strony w ramach Umowy.

§ 14. Postanowienia końcowe

1. Wszelkie zmiany Umowy wymagają formy pisemnego aneksu pod rygorem nieważności z wyjątkiem zmiany osób odpowiedzialnych za realizację Umowy, o których mowa w § 4 ust. 1-2 Umowy, kiedy wystarczające jest poinformowanie pisemnie drugiej strony.
2. Strony przewidują możliwość wprowadzenia zmian do Umowy w przypadku gdy:
 - 1) nastąpiła zmiana przepisów prawa powszechnie obowiązującego, która ma wpływ na termin lub zakres realizacji przedmiotu Umowy;
 - 2) w przypadku wystąpienia Siły Wyższej, o której mowa w § 7 Umowy;
 - 3) gdy niezbędna jest zmiana terminu wykonania Umowy z uwagi na wprowadzenie stanu zagrożenia epidemicznego, stanu epidemii, stanu wyjątkowego lub stanu klęski żywiołowej;
3. Strona wnosząca o zmianę Umowy, o której mowa w ust. 2, zobowiązana jest do przekazania na piśmie warunków zmiany wraz z uzasadnieniem w terminie 5 dni od daty zaistnienia okoliczności i proponowanego terminu wprowadzenia zmiany.
4. Strony ustalają, że w przypadku zaistnienia okoliczności, o których mowa w ust. 3, wprowadzenie zmiany możliwe będzie wyłącznie w określonym przez Zamawiającego wymiarze.
5. Wykonawca nie może przelać wierzytelności wynikających z Umowy na osoby trzecie bez pisemnej zgody Zamawiającego.
6. W okresie obowiązywania stanu zagrożenia epidemicznego, stanu epidemii, stanu wyjątkowego albo stanu klęski żywiołowej, wszelkie oświadczenia Stron, zawiadomienia, zgłoszenia dotyczące Umowy (w tym akceptacja Protokołu odbioru), w przypadku trudności z dochowaniem formy określonej w Umowie, mogą zostać złożone pocztą elektroniczną za pomocą e-maila. Za termin przekazania przyjmuje się datę dostarczenia e-maila na adresy wskazane w § 4.
7. W sprawach nieuregulowanych Umową mają zastosowanie przepisy Kodeksu cywilnego.

8. Spory wynikłe z Umowy rozstrzygać będzie sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
9. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, z których dwa otrzymuje Zamawiający a jeden Wykonawca.

§ 15. Załączniki do Umowy

Integralną część Umowy stanowią:

Załącznik nr 1 – Protokół odbioru przedmiotu umowy (wzór);

Załącznik nr 2 – Oferta Wykonawcy;

Załącznik nr 3 - Klauzula informacyjna RODO;

Załącznik nr 4 – Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych;

Załącznik nr 5 – Umowa powierzenia przetwarzania danych osobowych (wzór).

ZAMAWIAJĄCY

WYKONAWCA

*Na podstawie art. 54 ust 3, w zw. z art. 54 ust. 1 pkt 3 uofp
potwierdzam dokonanie kontroli wstępnej.*

.....
Główny księgowy

PROTOKÓŁ ODBIORU PRZEDMIOTU UMOWY
(wzór)

WYKONAWCA:

.....
.....

ZAMAWIAJĄCY:

GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208,
00-925 Warszawa

Sporządzony w dniu..... r., w Warszawie, na podstawie Umowy numer 38/DK/2023 z dnia.....
dotyczącej umowy o dotację pt. „.....”.

W odbiorze uczestniczyli:

Ze strony Wykonawcy:

imię i nazwisko

Ze strony Zamawiającego:

imię i nazwisko

imię i nazwisko

Przedstawiciel Wykonawcy przedstawił do odbioru przedmiot Umowy w zakresie:

Bony towarowe RTV/AGD o terminie ważności 24 miesięcy:

L.p.	Nominat [zł]	Liczba sztuk odebranych
1	50,00
2	100,00
	RAZEM:

I. Warunki odbioru:

1. W ramach realizacji Umowy Wykonawca wykonał przedmiot Umowy zgodnie z wymaganiami Zamawiającego.

*TAK - bez uwag.

*NIE uwagi:.....

2. Dostawa towaru odbyła się o godz.....**(należy wskazać godzinę dostawy)**

3. Przedmiot Umowy został dostarczony (**w terminie */ po terminie***) określonym w Umowie;
Zwłoka liczona od dnia**,

II. Zamawiający w stosunku do przedmiotu Umowy wskazuje następujące rozbieżności:

.....

III. Zamawiający wzywa do usunięcia wyżej wskazanych rozbieżności w terminie do:

.....

IV. Końcowy wynik odbioru:

1. Pozytywny**) – Zamawiający dokonuje odbioru przedmiotu Umowy objętego niniejszym protokołem bez zastrzeżeń i stwierdza, że został on wykonany w terminie, zgodnie z wymogami określonymi w Umowie.

2. Pozytywny z zastrzeżeniem**) – Zamawiający dokonuje odbioru przedmiotu Umowy objętego niniejszym protokołem stwierdza, że:
został on wykonany po terminie określonym w Umowie, zwłoka liczona jest od dnia

.....*;

W związku z powyższym naliczona zostanie kara umowna, o której mowa w §ust. pkt)
Umowy.**

3. Negatywny**) – Zamawiający odmawia odbioru przedmiotu Umowy objętego niniejszym protokołem w związku z rozbieżnościami ujętymi w pkt. II.

*- jeśli dotyczy,

** - niepotrzebne skreślić.

Niniejszy protokół sporządzono w trzech jednobrzmiących egzemplarzach, w tym jeden dla Zamawiającego i dwa dla Wykonawcy.

W imieniu Wykonawcy

W imieniu Zamawiającego

.....

.....

.....

.....

Imię i nazwisko

Imię i nazwisko

/pieczętka firmowa, data podpis/

/pieczętka firmowa, data podpis/

Oferta Wykonawcy

Informacje dotyczące przetwarzania danych osobowych w związku z realizacją umowy

W związku z realizacją wymogów 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)¹ (RODO), administrator informuje o zasadach oraz o przysługujących Pani/Panu prawach związanych z przetwarzaniem Pani/Pana danych osobowych.

I. Administrator

Administratorem Pani/Pana danych osobowych jest Główny Urząd Statystyczny z siedzibą al. Niepodległości 208, 00-925 Warszawa.

II. Inspektor ochrony danych

Z inspektorem ochrony danych (IOD) może się Pani/Pan kontaktować:

1. pocztą tradycyjną na adres: IOD GUS, al. Niepodległości 208, 00-925 Warszawa,
2. pocztą elektroniczną na adres e-mail: IODGUS@stat.gov.pl.

Do IOD należy kierować wyłącznie sprawy dotyczące przetwarzania Pani/Pana danych osobowych przez administratora, w tym realizacji Pani/Pana praw wynikających z RODO.

III. Cele oraz podstawa prawna przetwarzania Pani/Pana danych osobowych

Pani/Pana dane osobowe będą przetwarzane celem zawarcia i prawidłowej realizacji umowy 38/DK/2023.

Podstawą prawną przetwarzania danych jest:

- a) w zakresie osób będących Stroną Umowy:
 - art. 6 ust. 1 lit b RODO - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
 - art. 6 ust. 1 lit c RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze w związku z przepisami ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710, z późn. zm.), przepisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164, z późn. zm.), rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej (Dz. U. z 2019 poz. 246), przepisami ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902) oraz w związku z przepisami prawa podatkowego;
- b) w zakresie osób niebędących Stroną Umowy, ale biorących udział w jej realizacji oraz osób których dane Zamawiający uzyska od Wykonawcy na podstawie Umowy:
 - art. 6 ust. 1 lit c RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze w związku z przepisami ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, przepisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej, przepisami ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej oraz w związku z przepisami prawa podatkowego;
 - art. 6 ust. 1 lit. f RODO - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, to jest do umożliwienia prawidłowej realizacji umowy między Stronami.

IV. Odbiorcy danych osobowych

Odbiorcą Pani/Pana danych osobowych będą podmioty współpracujące z administratorem, w tym dostawcy usług

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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.)

technicznych i organizacyjnych umożliwiających wykonanie umowy oraz przechowywanie dokumentacji jej dotyczącej, osoby i podmioty upoważnione na podstawie przepisów prawa powszechnie obowiązującego.

V. Okres przechowywania danych osobowych

Pani/Pana dane osobowe będą przechowywane przez:

1. okres realizacji umowy oraz maksymalnie przez okres 6 letni od upływu daty wymagalności roszczenia cywilnoprawnego za zasadach określonych w ustawie z dnia z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. z 2022 r. poz. 1360, z późn. zm.);
2. po okresie, o którym mowa w pkt 1), w celach archiwalnych zgodnie z przepisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz w rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej.

VI. Prawa osoby, której dane osobowe dotyczą

Przysługuje Pani/Panu prawo do:

1. dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
2. sprostowania (poprawiania) danych osobowych;
3. do sprzeciwu wobec przetwarzania danych osobowych – w przypadku przetwarzania na podstawie art. 6 ust. 1 lit. f RODO;
4. ograniczenia przetwarzania danych osobowych;
5. wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (na adres Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa), jeżeli Pani/Pana zdaniem przetwarzanie Pani/Pana danych osobowych narusza przepisy RODO.

VII. Dobrowolność/ Obowiązek podania danych osobowych

Obowiązek podania danych osobowych dotyczących Strony umowy jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego oraz zawarciem i realizacją umowy. Konsekwencje niepodania danych osobowych wynikają z ustawy Pzp. Podanie danych osób niebędących Stroną Umowy, ale biorących udział w jej realizacji jest dobrowolne, jednakże niezbędne do realizacji celów, o których mowa w pkt III, a brak ich podania może wpłynąć na nieprawidłową realizację umowy.

VIII. Zautomatyzowane podejmowanie decyzji, w tym profilowanie

Pani/Pana dane osobowe nie będą profilowane ani też nie będą podlegały zautomatyzowanemu podejmowaniu decyzji.

IX. Przekazywanie danych do państwa trzeciego/organizacji międzynarodowej

Administrator danych nie ma zamiaru przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych

I. Słownik pojęć:

aktywa – wszystko, co ma wartość dla jednostek służb statystyki publicznej i z tego względu wymaga ochrony [na podstawie normy PN-ISO/IEC 27001];

jednostka – rozumiane rozdzielnie GUS i pozostałe jednostki służb statystyki publicznej;

komórka organizacyjna GUS – departament, biuro, wydział, samodzielne stanowisko pracy w Głównym Urzędzie Statystycznym;

jednostka służb statystyki publicznej – jednostki służb statystyki publicznej podległe i podporządkowane Prezesowi GUS (GUS, CBS, CIS, Zakład Wydawnictw Statystycznych, urzędy statystyczne oraz CBIeS);

Incydent bezpieczeństwa informacji – pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji [na podstawie normy PN ISO/IEC 27000];

Pełnomocnik ds. SZBI – dyrektor komórki organizacyjnej GUS właściwej ds. bezpieczeństwa informacji powołany przez Prezesa GUS na mocy zarządzenia wewnętrznego nr 8 Prezesa GUS z dnia 20 lutego 2020 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w statystyce publicznej [definicja własna];

System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne [na podstawie art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne];

Właściciel Aktywu – dyrektor komórki organizacyjnej GUS/dyrektor jssp;

II. Zasady zachowania poufności danych i informacji:

1. Kontrahenci i osoby z zewnątrz zobowiązują się do zachowania w poufności wszelkich danych i informacji, niezależnie od sposobu ich pozyskania (zamierzony lub przypadkowy) i bez względu na sposób i formę ich przekazania.
2. Obowiązek, o którym mowa w pkt 1, jeżeli przepisy prawa nie stanowią inaczej, obowiązuje przez okres 10 lat po jej rozwiązaniu, wygaśnięciu lub odstąpieniu od niej, bez względu na przyczynę.
3. Obowiązku zachowania poufności nie stosuje się do danych i informacji:
 - 1) dostępnych publicznie;
 - 2) otrzymanych zgodnie z przepisami prawa powszechnie obowiązującego, od osoby trzeciej bez obowiązku zachowania poufności;
 - 3) które w momencie ich przekazania były już znane kontrahentowi/ osobie z zewnątrz bez obowiązku zachowania poufności;
 - 4) w stosunku do których kontrahent/ osoba z zewnątrz uzyskał(a) pisemną zgodę na ich ujawnienie.
4. W przypadku, gdy ujawnienie wszelkich danych i informacji, co do których kontrahenci i osoby z zewnątrz zobowiązali się zachować w poufności jest wymagane na podstawie przepisów prawa powszechnie obowiązującego, kontrahent/ osoba z zewnątrz poinformuje osobę wskazaną do kontaktu o przyczynach i zakresie ujawnionych Informacji Poufnych. Poinformowanie takie powinno nastąpić w formie pisemnej lub w formie wiadomości wysłanej na adres poczty elektronicznej osoby wskazanej do kontaktu, chyba że takie poinformowanie byłoby sprzeczne z przepisami prawa powszechnie obowiązującego.
5. Kontrahent/ osoba z zewnątrz zobowiązuje się do niewykorzystywania Informacji Poufnych w celach innych niż cel, dla którego zostały mu ujawnione.
6. Kontrahent/ osoba z zewnątrz zobowiązuje się do dołożenia właściwych starań w celu zabezpieczenia Informacji Poufnych przed ich utratą, zniekształceniem oraz dostępem nieupoważnionych osób trzecich.
7. W przypadku utraty lub zniekształcenia Informacji Poufnych lub dostępu nieupoważnionej osoby trzeciej do Informacji Poufnych, Kontrahent/ osoba z zewnątrz bezzwłocznie podejmie odpowiednie do sytuacji działania ochronne oraz poinformuje osobę wskazaną do kontaktu o przyczynach i zakresie ujawnionych Informacji Poufnych. Poinformowanie takie powinno nastąpić w formie pisemnej lub w formie wiadomości wysłanej na

adres poczty elektronicznej osoby wskazanej do kontaktu, chyba że takie poinformowanie byłoby sprzeczne z przepisami prawa powszechnie obowiązującego.

III. **Ochrona danych osobowych**

1. Kontrahent/ osoba z zewnątrz zobowiązuje się przetwarzać powierzone dane osobowe zgodnie z określonym celem ich przetwarzania, rozporządzeniem RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą;
2. Kontrahent/ osoba z zewnątrz zobowiązuje się przed zawarciem Umowy wypełnić obowiązki informacyjne przewidziane w art. 13 lub art. 14 ogólnego rozporządzenia o ochronie danych (RODO) oraz w zakresie określonym w załączniku do Umowy wobec każdej osoby fizycznej, od której dane osobowe bezpośrednio lub pośrednio pozyskał w celu wpisania jej do treści Umowy, jako dane osoby reprezentującej go lub działającej w jego imieniu przy realizowaniu Umowy. Kontrahent/ osoba z zewnątrz zobowiązuje się w przypadku wyznaczenia lub wskazania do działania przy wykonywaniu Umowy osób innych niż wymienione w jej treści, najpóźniej wraz z przekazaniem danych osobowych tych osób, zrealizować obowiązki informacyjne w trybie art. 13 lub art. 14 RODO oraz określone w załączniku do Umowy.
3. W przypadku powierzenia przetwarzania danych osobowych kontrahentowi/ osobie z zewnątrz, wymaga się podpisania przez kontrahenta/ osobę z zewnątrz umowy powierzenia przetwarzania danych osobowych.
4. Umowy powierzenia muszą zawierać szczegółowe uregulowania w zakresie przetwarzania powierzonych danych osobowych i ich ochrony.

IV. **Bezpieczeństwo fizyczne i środowiskowe**

1. Obowiązuje zakaz wnoszenia na teren siedziby GUS jakichkolwiek materiałów niebezpiecznych, których posiadanie i przechowywanie jest zabronione prawem. W przypadku stwierdzenia ich obecności w pomieszczeniach, dyrektor komórki organizacyjnej GUS właściwej ds. administracyjnych lub dyrektor jednostki odpowiedzialny jest za doprowadzenie do ich usunięcia.
2. Wyróżnia się następujące obszary bezpieczne:
 - a) strefa chroniona (strefa administracyjna),
 - b) strefa zabezpieczona (strefa bezpieczeństwa);
3. Wydziela się obszar dostaw i załadunku. Dostęp do pomieszczeń magazynowych jest nadzorowany. Prowadzona jest kontrola ruchu osobowego i materiałowego.
4. Pomieszczenia, w których przetwarzane są informacje wrażliwe dla statystyki publicznej, są wyposażone w zamek mechaniczny lub elektroniczny.

Strefa chroniona (strefa administracyjna):

- 1) na granicach strefy chronionej (strefy administracyjnej) funkcjonuje kontrola dostępu (tripody lub czytniki na drzwiach);
- 2) wejście do strefy chronionej (strefy administracyjnej), kontrahenta/ osoby z zewnątrz wymaga wydania identyfikatora i jego zaewidencjonowania. Ewidencjonowanie wejść do strefy chronionej (strefy administracyjnej) odbywa się poprzez dokonanie przez ochronę/recepcję lub wyznaczonego pracownika wpisu w ewidencji wejść i wyjść do strefy chronionej (strefy administracyjnej) oraz wydanie identyfikatora/karty magnetycznej typu „Gość”;
- 3) za wszelkie naruszenia bezpieczeństwa informacji przez osoby, które uzyskały dostęp do strefy chronionej (strefy administracyjnej) odpowiada dyrektor komórki organizacyjnej GUS/ dyrektor jednostki lub pracownik wnioskujący o przyznanie identyfikatora typu „Gość”;
- 4) osoby, bądź przedstawiciele podmiotów zewnętrznych świadczących usługi, w szczególności kurierzy, zaopatrzeniowcy, serwisanci poruszają się w granicy strefy chronionej (strefy administracyjnej) wyłącznie pod nadzorem wyznaczonego pracownika;
- 5) szczegóły dotyczące wejścia do strefy chronionej GUS określone zostały w zarządzeniu Dyrektora Generalnego GUS w sprawie „Zasad organizacji ruchu osób i pojazdów oraz zabezpieczenia budynku i mienia Głównego Urzędu Statystycznego”.

Strefa zabezpieczona (strefa bezpieczeństwa):

- 1) strefa zabezpieczona (strefa bezpieczeństwa) to wydzielona część strefy chronionej (strefy administracyjnej) wyposażona w dodatkowe, niezależne systemy zabezpieczeń. Rodzaj zabezpieczeń określa Właściciel aktywów przechowywanych w danym pomieszczeniu, stosownie do ich rodzaju i wartości;

- 2) zasoby znajdujące się w strefie zabezpieczonej (strefie bezpieczeństwa) podlegają szczególnej ochronie i są zabezpieczone przed pożarem;
- 3) strefy zabezpieczone (strefy bezpieczeństwa) posiadają zabezpieczenia zapewniające ochronę nośników informacji. Serwerownie wyposażone są w system sygnalizujący wystąpienie pożaru oraz system klimatyzacji. Strefy zabezpieczone (strefy bezpieczeństwa) są chronione systemem sygnalizacji włamania i napadu oraz wyposażone w urządzenia pozwalające na alarmowe powiadomienie obsługi i ochrony. System sygnalizacji napadu i włamania zapewnia skuteczne przekazanie sygnału o realnym zagrożeniu do wskazanych osób, miejsc i urządzeń;
- 4) wstęp do strefy zabezpieczonej (strefy bezpieczeństwa) jest ograniczony tylko do osób, które uzyskały stosowne uprawnienia wydane przez Właściciela aktywów przechowywanych w danym pomieszczeniu. Wejście oraz wyjście ze stref bezpieczeństwa rejestrowane jest przez system kontroli dostępu lub wyznaczonego przez Właściciela aktywów przechowywanych w danym pomieszczeniu pracownika. Wyznaczony pracownik rejestruje tożsamość osób oraz czas ich wejścia i wyjścia;
- 5) dopuszcza się przebywanie kontrahenta i osób z zewnątrz bez uprawnień dostępu do strefy zabezpieczonej (strefy bezpieczeństwa) tylko w wyjątkowych przypadkach, w celu wykonania działań serwisowych i innych określonych w regulacjach wewnętrznych (audyt), za zezwoleniem Właściciela aktywów przechowywanych w danym pomieszczeniu. Przebywanie osób bez uprawnień dostępu do strefy zabezpieczonej (strefy bezpieczeństwa) możliwe jest wyłącznie pod nadzorem pracownika, który posiada uprawnienia dostępu do danej strefy;
- 6) wnoszenie i wnoszenie do i ze strefy zabezpieczonej (strefy bezpieczeństwa) elektronicznych nośników informacji jest uzasadnione (np.: wynikające z procedury dot. kaset backup) lub nadzorowane;
- 7) w strefie zabezpieczonej (strefie bezpieczeństwa) zabronione jest korzystanie z urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających, np. kamer w urządzeniach mobilnych w celu rejestracji obrazu lub dźwięku bez pisemnej zgody Właściciela aktywów przechowywanych w danym pomieszczeniu lub wyznaczonego przez niego pracownika.

V. Dostęp do zasobów systemów teleinformatycznych

1. Dostęp do systemu teleinformatycznego uzyskuje wyłącznie uprawniony kontrahent/osoba z zewnątrz. Dostęp jest indywidualnie zdefiniowany. Kontrahent/ osoba z zewnątrz ma dostęp jedynie do zasobów, które są niezbędne.
2. Kontrola dostępu dla kontrahenta/ osoby z zewnątrz do systemu teleinformatycznego realizowana jest poprzez mechanizmy uwierzytelniania.
3. Kontrahent/osoba z zewnątrz uzyskują uprawnienia w zakresie korzystania z systemu teleinformatycznego na wniosek Właściciela aktywów. Nie dotyczy to organów umocowanych prawnie.
4. Uprawnienia dla kontrahenta/osoby z zewnątrz nie mogą być przyznane na czas nieokreślony i podlegają aktualizacji co 90 dni.
5. Warunki korzystania z połączenia wewnętrznej sieci statystyki publicznej z systemami zewnętrznymi regulują podpisane umowy, szczególnie precyzyjne warunki techniczne i funkcjonalne połączenia.

VI. Dostęp do zasobów z sieci innych instytucji

1. Kontrahent/osoba z zewnątrz otrzymują dostęp do sieci teleinformatycznej na mocy przepisów prawa.
2. Kontrahent/osoba z zewnątrz mogą uzyskać uprawnienia w zakresie korzystania z systemu teleinformatycznego na wniosek Właściciela aktywów. Nie dotyczy to organów umocowanych prawnie;
3. Wniosek o dostęp do sieci statystyki publicznej powinien zawierać informacje o celu podłączenia, przewidywanej liczbie podłączonych stanowisk i użytkowników, metodzie zabezpieczenia przed nieautoryzowanym dostępem i używanym antywirusie.
4. Przed wydaniem decyzji o zgodzie na podłączenie do sieci statystyki publicznej, Prezes GUS zasięga opinii Pełnomocnika ds. SZBI.
5. Specyfikacja techniczna połączenia jest załącznikiem do porozumienia lub zawieranej umowy.
6. Specyfikacja powinna zawierać w szczególności następujące ustalenia:
 - a) szyfrowane połączenie powinno być zabezpieczone odpowiednim certyfikatem,
 - b) zestawione połączenie powinno być jedynie między ściśle określonymi adresami IP podłączanej sieci oraz ściśle określonymi adresami IP sieci wewnętrznej statystyki publicznej oraz dla ściśle określonych portów przypisanych do adresów w sieci teleinformatycznej statystyki publicznej,

- c) każdorazowe zestawienie połączenia między podłączaną siecią teleinformatyczną podmiotu zewnętrznego, a siecią teleinformatyczną statystyki publicznej należy autoryzować loginem i hasłem lub certyfikatem oraz logowaniem,
 - d) zasoby udostępniane użytkownikom z innych instytucji obejmują wyłącznie dostęp do aplikacji. Nie mogą być udostępniane takie zasoby jak serwery plików lub poczta elektroniczna;
7. Właściciel aktywu zatwierdza uprawnienia użytkowników z innych instytucji do danej aplikacji będącej w zasobach statystyki publicznej. Użytkownicy z innych instytucji nie mogą posiadać praw administracyjnych;

VII. Ochrona przed szkodliwym oprogramowaniem i kodem mobilnym

1. Wszystkie elektroniczne nośniki informacji dostarczone z zewnątrz do siedziby GUS są dopuszczone do używania po wcześniejszym sprawdzeniu ich programem antywirusowym na komputerze odizolowanym od sieci GUS.
2. Wszystkie pliki przed wysłaniem pocztą elektroniczną lub przekazaniem stronom trzecim (kontrahentowi/osobie zewnętrznej) są testowane oprogramowaniem antywirusowym.

VIII. Odbiór systemu

1. Przed przekazaniem do użytkownika oprogramowania opracowanego na rzecz statystyki publicznej, osoby je opracowujące muszą usunąć wszystkie specjalne ścieżki dostępu tak, aby dostęp był możliwy jedynie z zastosowaniem zasad bezpieczeństwa informacji. Oznacza to, że muszą być usunięte wszystkie nieudokumentowane funkcje pozwalające ominąć system zabezpieczeń. Muszą zostać również usunięte wszystkie uprawnienia systemowe ustanowione dla potrzeb prowadzenia prac nad oprogramowaniem, lecz zbędne w środowisku produkcyjnym. Powinno to być udokumentowane oświadczeniem kontrahenta, w którym potwierdza usunięcie powyższych nadmiarowych funkcjonalności.
2. W przypadku podjęcia decyzji o przechowywaniu kodu źródłowego pisanego na zamówienie statystyki publicznej poza siedzibą GUS, konieczne jest zawarcie umów depozytowych dotyczących takiego kodu źródłowego z podmiotami niezależnymi od dostawcy oprogramowania. Umowy te powinny określać niezależny podmiot, któremu twórca oprogramowania dostarczy kod źródłowy i wszystkie jego aktualizacje. Powinny też określać sytuacje, w których kod źródłowy zostanie udostępniony statystyce publicznej, jak na przykład upadłość lub likwidacja dostawcy oprogramowania lub niewywiązywanie się przez niego z postanowień umowy dotyczących aktualizacji oprogramowania.

IX. Naruszenia bezpieczeństwa informacji oraz wnioski dotyczące bezpieczeństwa informacji

1. Zasady bezpieczeństwa informacji obowiązują wszystkich kontrahentów i osoby z zewnątrz, które otrzymują dostęp do zasobów informacyjnych statystyki publicznej.
2. Kontrahenci i osoby z zewnątrz mający dostęp do zasobów informacyjnych na podstawie odrębnych przepisów/ upoważnień, przed przyznaniem dostępu do zasobów informacyjnych otrzymują do zapoznania się *Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych*.
3. Odpowiedzialność za bezpieczeństwo informacji statystyki publicznej obejmuje działania, które miały miejsce w siedzibie GUS oraz wszelkie sytuacje, w których informacje związane z działalnością są przetwarzane poza jej siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci teleinformatycznej statystyki publicznej.
4. Kontrahent i osoba z zewnątrz mają obowiązek zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, procedury i instrukcje dotyczące bezpieczeństwa informacji do osoby wskazanej do kontaktu, która przekazuje te informacje do Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni w jssp, w którym aktualnie realizowane są przez nich zadania rzecz statystyki.
5. Każdy incydent związany z bezpieczeństwem informacji w GUS, CIS, ZWS i CBS powinien być zgłoszony natychmiast po jego wykryciu.
6. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji przez pracowników statystyki publicznej odbywa się przez dedykowaną stronę www (<http://serwisdesk>), e-mailem: serwisdesk@stat.gov.pl bądź, w godzinach pracy urzędu, telefonicznie (22 608 3689);
7. W przypadku zmian w przepisach Wymagań, kontrahent i osoba z zewnątrz zostaną o tym poinformowani na piśmie.

**Umowa powierzenia przetwarzania
danych osobowych
38/DK/2023**

SEKCJA I

Klauzula 1

Cel i zakres

1. Celem niniejszych standardowych klauzul umownych („klauzule”) jest zapewnienie przestrzegania art. 28 ust. 3 i 4 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) – dalej rozporządzenie (UE) 2016/679.
2. Administratorzy i podmioty przetwarzające wymienieni w załączniku I uzgodnili niniejsze klauzule w celu zapewnienia przestrzegania art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679.
3. Niniejsze klauzule mają zastosowanie do przetwarzania danych osobowych określonego w załączniku II.
4. Załączniki I–IV stanowią integralną część klauzul.
5. Niniejsze klauzule pozostają bez uszczerbku dla obowiązków, którym podlega administrator danych na mocy rozporządzenia (UE) 2016/679.
6. Niniejsze klauzule same w sobie nie zapewniają wypełnienia obowiązków związanych z międzynarodowym przekazywaniem danych zgodnie z rozdziałem V rozporządzenia (UE) 2016/679.

Klauzula 2

Niezmiennosc klauzul

- a) Strony zobowiązują się nie zmieniać klauzul z wyjątkiem dodawania informacji do załączników lub aktualizowania zawartych w nich informacji.
- b) Postanowienie to nie uniemożliwia stronom umieszczania standardowych klauzul umownych określonych w niniejszych klauzulach w treści umowy o szerszym zakresie ani dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem, że nie będą one bezpośrednio lub pośrednio sprzeczne z klauzulami umownymi, ani nie będą naruszały podstawowych praw lub wolności osób, których dane dotyczą.

Klauzula 3

Wykładnia

- a) Jeżeli w niniejszych klauzulach użyto terminów zdefiniowanych odpowiednio w rozporządzeniu (UE) 2016/679, terminy te mają takie samo znaczenie jak w tych rozporządzeniach.
- b) Niniejsze klauzule odczytuje się i interpretuje w świetle przepisów rozporządzenia (UE) 2016/679.
- c) Niniejszych klauzul nie interpretuje się w sposób sprzeczny z prawami i obowiązkami przewidzianymi w rozporządzeniu (UE) 2016/679, ani w sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.

Klauzula 4

Hierarchia

W razie sprzeczności między niniejszymi klauzulami a postanowieniami powiązanych umów między stronami istniejących w chwili uzgadniania niniejszych klauzul lub zawartych po ich uzgodnieniu, pierwszeństwo mają niniejsze klauzule.

SEKCJA II

OBOWIĄZKI STRON

Klauzula 6

Opis przetwarzania

Szczegóły dotyczące operacji przetwarzania, w szczególności kategorie danych osobowych i cele, dla których dane osobowe są przetwarzane w imieniu administratora, określono w załączniku II.

Klauzula 7

Obowiązki stron

7.1. Polecenia

- 1) Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane.
- 2) Podmiot przetwarzający bezzwłocznie powiadamia administratora, jeżeli w opinii podmiotu przetwarzającego polecenie wydane przez administratora narusza rozporządzenie (UE) 2016/679 lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.

7.2. Ograniczenie celu

Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnym celu lub celach przetwarzania, określonych w załączniku II, chyba że otrzyma dalsze polecenia od administratora.

7.3. Czas trwania przetwarzania danych osobowych

Przetwarzanie przez podmiot przetwarzający odbywa się wyłącznie przez okres określony w załączniku II.

7.4. Bezpieczeństwo przetwarzania

- a) W celu zapewnienia bezpieczeństwa danych osobowych podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w załączniku III. Zapewnienie bezpieczeństwa danych obejmuje ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych). Oceniając odpowiedni poziom bezpieczeństwa, strony należyście uwzględniają stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz związane z tym ryzyko dla osób, których dane dotyczą.
- b) Podmiot przetwarzający udziela członkom swojego personelu dostępu do danych osobowych podlegających przetwarzaniu jedynie w zakresie bezwzględnie niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

7.5. Dane wrażliwe

Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane

genetyczne lub dane biometryczne do celów jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby, bądź dane dotyczące wyroków skazujących i czynów zabronionych („dane wrażliwe”), podmiot przetwarzający stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia.

7.6. Dokumentacja i zgodność

- a) Strony są w stanie wykazać zgodność z niniejszymi klauzulami.
- b) Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszymi klauzulami.
- c) Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, które są określone w niniejszych klauzulach i wynikają bezpośrednio z rozporządzenia (UE) 2016/679. Na wniosek administratora podmiot przetwarzający zezwala również na audyty czynności przetwarzania objętych niniejszymi klauzulami i uczestniczy w tych audytach. Audyty te przeprowadza się w rozsądnych odstępach czasu lub jeżeli istnieją przesłanki wskazujące na niezgodność. Podejmując decyzję w sprawie przeglądu lub audytu, administrator może wziąć pod uwagę odpowiednie certyfikaty, jakie ma podmiot przetwarzający.
- d) Administrator może przeprowadzić audyt samodzielnie lub upoważnić do jego przeprowadzenia niezależnego audytora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego. Audyty te przeprowadza się, informując o nich, w stosownych przypadkach, z odpowiednim wyprzedzeniem.
- e) Na wniosek właściwego(-ych) organu(-ów) nadzorczego(-ych) strony udostępniają mu (im) informacje, o których mowa w niniejszej klauzuli, w tym wyniki wszelkich audytów.

7.7. Korzystanie z usług podmiotów podprzetwarzających

- a) **UPRZEDNIA SZCZEGÓŁOWA ZGODA:** Podmiot przetwarzający nie może podzlecać żadnych operacji przetwarzania dokonywanych w imieniu administratora zgodnie z niniejszymi klauzulami podmiotowi podprzetwarzającemu bez uprzedniej szczegółowej pisemnej zgody administratora. Podmiot przetwarzający składa wniosek o udzielenie szczegółowej zgody co najmniej 14 dni przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego wraz z informacjami niezbędnymi do tego, by administrator mógł podjąć decyzję w sprawie zgody. Załącznik IV zawiera wykaz podmiotów podprzetwarzających upoważnionych przez administratora. Strony są obowiązane do aktualizacji załącznika IV.
- b) Jeżeli podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), dokonuje tego w drodze umowy, która nakłada na podmiot podprzetwarzający zasadniczo takie same obowiązki w zakresie ochrony danych jak obowiązki nałożone na podmiot przetwarzający dane zgodnie z niniejszymi klauzulami. Podmiot przetwarzający zapewnia, aby podmiot podprzetwarzający wypełniał obowiązki, którym podlega podmiot przetwarzający na mocy niniejszych klauzul oraz rozporządzenia (UE) 2016/679.
- c) Na wniosek administratora podmiot przetwarzający przekazuje administratorowi kopię umowy, jaką zawarł z podmiotem podprzetwarzającym, a w razie wprowadzenia zmian przekazuje administratorowi jej zaktualizowaną wersję. W zakresie niezbędnym do ochrony tajemnicy handlowej lub innych informacji poufnych, w tym danych osobowych, podmiot przetwarzający może utajnić tekst umowy przed jej udostępnieniem.
- d) Podmiot przetwarzający pozostaje w pełni odpowiedzialny przed administratorem za wykonanie obowiązków podmiotu podprzetwarzającego zgodnie z jego umową z podmiotem przetwarzającym. Podmiot przetwarzający powiadamia administratora o każdym przypadku niewywiązania się przez podmiot podprzetwarzający z jego zobowiązań umownych.
- e) Podmiot przetwarzający uzgadnia z podmiotem podprzetwarzającym klauzulę dotyczącą beneficjenta będącego osobą trzecią, zgodnie z którą to klauzulę – jeżeli podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub stanie się niewypłacalny – administrator ma prawo rozwiązać umowę z podmiotem podprzetwarzającym i nakazać mu usunięcie lub zwrot danych osobowych.

7.8. Międzynarodowe przekazywanie danych

a) Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie administratora lub w celu spełnienia szczególnego wymogu na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający, i odbywa się zgodnie z rozdziałem V rozporządzenia (UE) 2016/679.

b) Jeżeli zgodnie z klauzulą 7.7 podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), które wiążą się z przekazywaniem danych osobowych w rozumieniu rozdziału V rozporządzenia (UE) 2016/679, administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V rozporządzenia (UE) 2016/679 za pomocą standardowych klauzul umownych przyjętych przez Komisję zgodnie z art. 46 ust. 2 rozporządzenia (UE) 2016/679, pod warunkiem że spełnione są warunki stosowania tych standardowych klauzul umownych.

Klauzula 8

Pomoc dla administratora

1. Podmiot przetwarzający niezwłocznie zawiadamia administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na taki wniosek samodzielnie, chyba że administrator wyraził na to zgodę.
2. Podmiot przetwarzający pomaga administratorowi w wypełnianiu jego obowiązków dotyczących udzielania odpowiedzi na wnioski osób, których dane dotyczą, o skorzystanie z przysługujących im praw, z uwzględnieniem charakteru przetwarzania. Wypełniając swoje obowiązki zgodnie z lit. a) i b), podmiot przetwarzający stosuje się do poleceń administratora.
3. Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie z klauzulą 8 lit. b) podmiot przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje podmiot przetwarzający:
4. obowiązek przeprowadzenia oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych („ocena skutków dla ochrony danych”), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;
5. obowiązek skonsultowania się z właściwym(-i) organem(-ami) nadzorczym(-i) przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu jego ograniczenia;
6. obowiązek zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie administratora, jeżeli podmiot przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne;
7. obowiązki określone w art. 32 rozporządzenia (UE) 2016/679.
8. Strony określają w załączniku III odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać administratorowi w stosowaniu niniejszej klauzuli, jak również zakres wymaganej pomocy.

Klauzula 9

Zgłaszanie naruszenia ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający współpracuje z administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679 z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje podmiot przetwarzający.

9.1. Naruszenie ochrony danych dotyczące danych przetwarzanych przez administratora

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający wspomaga administratora:

- a) przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu(-ym) organowi(-om) nadzorcemu(-ym) niezwłocznie po tym, jak administrator dowiedział się o naruszeniu, w stosownych przypadkach/(chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);
- b) przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 rozporządzenia (UE) 2016/679 powinny być zawarte w zgłoszeniu administratora i obejmować co najmniej:
 - 1) charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
 - 2) możliwe konsekwencje naruszenia ochrony danych osobowych;
 - 3) środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
- c) Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki;
- d) przy wypełnianiu – zgodnie z art. 34 rozporządzenia (UE) 2016/679 – obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

9.2. Naruszenie ochrony danych dotyczące danych przetwarzanych przez podmiot przetwarzający

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez podmiot przetwarzający podmiot przetwarzający zgłasza naruszenie administratorowi niezwłocznie po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać co najmniej:

- a) opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);
- b) dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
- c) wskazanie prawdopodobnych konsekwencji naruszenia oraz środków, które zostały lub mają zostać wprowadzone w celu zaradzenia naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.

Strony określają w załączniku III wszystkie inne elementy, które ma przedstawić podmiot przetwarzający, wspomagając administratora w wypełnianiu jego obowiązków określonych w art. 33 i 34 rozporządzenia (UE) 2016/679.

SEKCJA III

POSTANOWIENIA KOŃCOWE

Klauzula 10

Naruszenie klauzul i rozwiązanie umowy

- a) Bez uszczerbku dla przepisów rozporządzenia (UE) 2016/679, w przypadku gdy podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszych klauzul, administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy podmiot przetwarzający zapewni zgodność z niniejszymi klauzulami, lub umowa ulega rozwiązaniu. Podmiot przetwarzający niezwłocznie zawiadamia administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszych klauzul.

- b) Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli:
1. administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z lit. a) i jeżeli zgodność z niniejszymi klauzulami nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;
 2. podmiot przetwarzający poważnie lub stale narusza niniejsze klauzule lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679;
 3. podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego(-ych) organu(-ów) nadzorczego(-ych) dotyczącej jego obowiązków wynikających z niniejszych klauzul lub z rozporządzenia (UE) 2016/679.
- c) Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli po zawiadomieniu administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie z klauzulą 7.1 lit. b), administrator nalega na wypełnienie polecenia.
- d) Po rozwiązaniu umowy podmiot przetwarzający, zależnie od decyzji administratora, usuwa wszystkie dane osobowe przetwarzane w imieniu administratora i poświadcza administratorowi, że tego dokonał, lub zwraca administratorowi wszystkie dane osobowe i usuwa istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Podmiot przetwarzający zapewnia przestrzeganie niniejszych klauzul do czasu usunięcia lub zwrotu danych.

Wykaz stron

Administrator (administratorzy):

Imię i nazwisko lub nazwa:

Adres:

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

Dane identyfikacyjne i kontaktowe inspektora ochrony danych:, e-mail

Podpis i data przystąpienia:

Podmiot przetwarzający (podmioty przetwarzające): *[dane identyfikacyjne i kontaktowe podmiotu przetwarzającego (podmiotów przetwarzających) oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez podmiot przetwarzający]*

1. **Imię i nazwisko lub nazwa:**

Adres:

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

Dane identyfikacyjne i kontaktowe inspektora ochrony danych:

Podpis i data przystąpienia:

ZAŁĄCZNIK II
Opis przetwarzania

PODMIOT PRZETWARZAJĄCY:

Kategorie osób, których dane osobowe są przetwarzane:

Kategorie przetwarzanych danych osobowych:/do uzupełnienia na etapie podpisywania umowy/.....

Przetwarzane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla personelu, który odbył specjalistyczne szkolenie), prowadzenie rejestru dostępu do danych, ograniczenia dotyczące dalszego przekazywania danych lub dodatkowe środki bezpieczeństwa:

Charakter przetwarzania:

Cel(e), w którym(-ych) dane osobowe są przetwarzane w imieniu administratora:

Czas trwania przetwarzania:

/W przypadku przetwarzania przez podmioty przetwarzające lub podprzetwarzające należy również określić przedmiot, charakter i czas trwania przetwarzania./

PODPRZETWARZAJĄCY:

Kategorie osób, których dane osobowe są przetwarzane:

.....

Kategorie przetwarzanych danych osobowych:

.....

Przetwarzane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla personelu, który odbył specjalistyczne szkolenie), prowadzenie rejestru dostępu do danych, ograniczenia dotyczące dalszego przekazywania danych lub dodatkowe środki bezpieczeństwa:

.....

Charakter przetwarzania:

.....

Cel(e), w którym(-ych) dane osobowe są przetwarzane w imieniu administratora:

.....

Czas trwania przetwarzania:

.....

ZAŁĄCZNIK III

Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych

UWAGA WYJAŚNIAJĄCA: Środki techniczne i organizacyjne należy opisać szczegółowo, a nie w sposób ogólny. Opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający (podmioty przetwarzające) (w tym wszelkie stosowne certyfikaty) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych. Przykłady możliwych środków: Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych Środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania Środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego Procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania Środki umożliwiające identyfikację i autoryzację użytkowników Środki zapewniające ochronę danych w czasie ich przekazywania Środki zapewniające ochronę danych w czasie ich przechowywania Środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe Środki umożliwiające rejestrowanie zdarzeń Środki służące do konfiguracji systemu, w tym konfiguracji domyślnej Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT Środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów Środki zapewniające minimalizację danych Środki zapewniające odpowiednią jakość danych Środki zapewniające ograniczone zatrzymywanie danych Środki zapewniające rozliczalność Środki umożliwiające przenoszenie danych i zapewnienie ich usuwania] W przypadku przekazywania danych podmiotom przetwarzającym lub podprzetwarzającym należy również opisać konkretne środki techniczne i organizacyjne, jakie powinien zastosować podmiot przetwarzający lub podprzetwarzający, aby móc udzielić pomocy administratorowi. Opis konkretnych środków technicznych i organizacyjnych, jakie powinien zastosować podmiot przetwarzający, aby móc udzielić pomocy administratorowi.

1) Opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający (podmioty przetwarzające) i podmiot/y podprzetwarzający/e (w tym wszelkie stosowne certyfikaty) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych:

1. PODMIOT PRZETWARZAJĄCY:

Opis technicznych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający oraz podmiot podprzetwarzający:

a)

Opis organizacyjnych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający oraz podmiot podprzetwarzający:

a)

/W przypadku przetwarzania przez podmioty przetwarzające lub podprzetwarzające należy również opisać techniczne i organizacyjne środki bezpieczeństwa./

2. PODPRZETWARZAJĄCY:

Opis technicznych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający oraz podmiot podprzetwarzający:

a)

Opis organizacyjnych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający oraz podmiot podprzetwarzający:

a)

ZAŁĄCZNIK IV

Wykaz podmiotów podprzetwarzających

UWAGA WYJAŚNIAJĄCA:

Niniejszy załącznik należy wypełnić w razie udzielenia szczegółowej zgody na korzystanie z usług podmiotów podprzetwarzających (klauzula 7.7 lit. a), opcja 1).

Administrator zezwolił na korzystanie z usług następujących podmiotów podprzetwarzających:

1. Imię i nazwisko lub nazwa:

.....

Adres:

.....

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

.....

Dane identyfikacyjne i kontaktowe inspektora ochrony danych:

.....

Opis zakresu podpowierzenia (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających):

a)

b)