|  |  |
| --- | --- |
| **Umowa powierzenia danych osobowych do przetwarzania** | |
|  |  |
| zawarta w dniu | ………………………………………….. w …………………… |
|  |  |
| pomiędzy | Górnośląsko-Zagłębiowską Metropolią  NIP: 634-290-18-73,  zwaną dalej w treści umowy „**Administratorem**” |
|  |  |
| reprezentowaną przez | 1 ...……………………………………………………………………………  2 …………………………………………………………………………….. |
|  |  |
| z siedzibą | ul. Barbary 21A, 40-053 Katowice |
|  |  |
| a | ……………………………………………………………………  reprezentowaną przez:  1. ………………………………………………………………………  2. ………………………………………………………………………  zwanym w treści umowy ” **Procesorem**”,  zwanymi również łącznie, jako „Strony”. |
|  |  |
| na podstawie | art. 28 ust. 3 i ust. 9 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). |
|  |  |
| dotycząca | powierzenia przetwarzania danych osobowych. |
|  |  |

**§ 1**

**Definicje**

Dla potrzeb niniejszej umowy, Strony ustalają następujące znaczenie niżej wymienionych pojęć:

1. **Dane osobowe** – dane w rozumieniu art. 4 pkt 1) RODO, tj. informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej, powierzone Procesorowi przez Administratora zgodnie z zakresem określonym w Umowie;
2. **Przetwarzanie Danych osobowych** – wszelkie operacje lub zestaw operacji wykonywanych na Danych Osobowych lub zestawach Danych osobowych, w sposób zautomatyzowany lub niezautomatyzowany takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
3. **Umowa** – niniejsza umowa powierzenia danych osobowych do przetwarzania;
4. **Umowa główna** – umowa nr…………., dotycząca ŚKUP 1.5 - Unowocześnienie systemu pobierania opłat za przejazdy publicznym transportem zbiorowym, zawarta przez Strony w dniu ………………
5. **RODO** - 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)

**§ 2**

**Oświadczenia Stron**

1. Administrator oświadcza, że jest uprawniony do powierzenia Procesorowi Danych osobowych do przetwarzania na podstawie niniejszej Umowy.
2. Strony oświadczają, że niniejsza Umowa została zawarta w celu wykonania obowiązków, o których mowa w RODO, w związku z zawarciem Umowy głównej.
3. Procesor oświadcza, iż dysponuje odpowiednimi środkami technicznymi i organizacyjnymi, doświadczeniem, wiedzą i wykwalifikowanym personelem, umożliwiającymi mu prawidłowe wykonanie niniejszej Umowy, spełnienie wymogów RODO oraz gwarantuje ochronę praw osób, których dane dotyczą.
4. Procesor na potwierdzenie gwarancji, o których mowa w ust. 3 zobowiązuje się do przestrzegania zasad zgodnie z opisem wdrożonych mechanizmów zapewniających bezpieczeństwo Przetwarzania Danych osobowych, stanowiący załącznik nr 1 do niniejszej Umowy,

**§ 3**

**Przedmiot Umowy oraz zakres, charakter i cel Przetwarzania Danych osobowych**

1. Administrator powierza Procesorowi do Przetwarzania Dane osobowe, a Procesor zobowiązuje się do zgodnego z prawem i niniejszą Umową ich przetwarzania, w celu określonym niniejszą Umową.
2. Zakres powierzonych do Przetwarzania Danych osobowych obejmuje dane szczegółowo określone w załączniku nr 2 do niniejszej Umowy, tj. dane w zakresie niezbędnym do realizacji Umowy głównej*.*
3. Przetwarzanie Danych osobowych odbywa się w formie papierowej lub przy wykorzystaniu systemów informatycznych.
4. Celem Przetwarzania Danych osobowych jest realizacja zadań, o których mowa w Umowie głównej.

**§ 4**

**Zasady Przetwarzania Danych osobowych**

1. Procesor może Przetwarzać Dane osobowe wyłącznie w zakresie i celu przewidzianym w Umowie.
2. Procesor zobowiązuje się Przetwarzać Dane osobowe zgodnie z udokumentowanym poleceniem Administratora, zawartym w Umowie, Umowie głównej lub w innym dokumencie wydanym przez Administratora, co dotyczy także przekazywania danych do państwa trzeciego lub organizacji międzynarodowej.
3. Procesor informuje Administratora przed podjęciem przetwarzania polegającego na przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, jeśli wynika ono z obowiązku nałożonego na niego przez przepisy prawa Unii lub prawa krajowego, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
4. Przy Przetwarzaniu Danych osobowych, Procesor powinien przestrzegać zasad wskazanych w niniejszej Umowie oraz RODO.
5. Procesor podejmuje środki zabezpieczające Dane osobowe, w szczególności obowiązany jest:
6. wdrożyć odpowiednie środki techniczne i organizacyjne, by Przetwarzanie Danych osobowych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, w tym środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzania, o którym mowa w art. 32 RODO a przede wszystkim powinien zabezpieczyć dane przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do Danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
7. pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32−36 RODO, w szczególności Procesor zobowiązuje się przekazywać Administratorowi informacje dotyczące stosowanych środków zabezpieczania Danych osobowych,
8. współpracować z Administratorem w sytuacji naruszenia ochrony Danych osobowych:
   * 1. niezwłocznie informować Administratora o podejrzeniach lub stwierdzonych przypadkach naruszenia ochrony Danych osobowych, nie później niż w 24 godziny od powzięcia takiej informacji,
     2. współpracować przy ocenie naruszenia i ewentualnym zawiadamianiu o tym organu nadzorczego lub osób, których Dane osobowe dotyczą,
     3. przekazywać informacje niezbędne Administratorowi do przeprowadzenia oceny skutków dla ochrony danych oraz przeprowadzania uprzednich konsultacji z organem nadzorczym i wdrożenia zaleceń organu,
     4. umożliwiać Administratorowi uczestnictwo w czynnościach wyjaśniających i informować Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia, przy czym powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru.
9. pomagać Administratorowi w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO;
10. niezwłocznie informować Administratora, jeżeli zdaniem Procesora wydane mu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie Danych osobowych;
11. stosować się do ewentualnych wskazówek lub zaleceń, wydanych przez krajowy organ nadzorczy lub Europejską Radę Ochrony Danych, dotyczących Przetwarzania Danych osobowych, w szczególności w zakresie stosowania RODO;
12. dopuszczać do Przetwarzania Danych osobowych, w szczególności do urządzeń w ramach których Dane osobowe są przetwarzane, wyłącznie osoby działające z jego upoważnienia, w zakresie wydanych przez Administratora udokumentowanych poleceń i przeszkolone z zakresu ochrony danych osobowych;
13. zapewnić, aby osoby upoważnione do Przetwarzania Danych osobowych zobowiązały się do zachowania tych danych oraz sposobów ich zabezpieczeń w tajemnicy, lub zapewnić by osoby podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, przy czym obowiązek zachowania tajemnicy istnieje również po realizacji Umowy lub ustaniu zatrudnienia u Procesora;
14. prowadzić rejestr kategorii czynności przetwarzania dokonywanych w imieniu Administratora, o którym mowa w art. 30 RODO, o ile dotyczy.
15. Procesor nie może skorzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej pisemnej zgody Administratora.
16. Procesor może skorzystać z usług innego podmiotu przetwarzającego pod warunkiem (i) zawarcia przez Procesora z tym podmiotem umowy zawierającej zapisy analogiczne do niniejszej Umowy oraz (ii) po wyrażeniu zgody lub niewyrażeniu sprzeciwu przez Administratora na takie dalsze powierzenie Danych osobowych do przetwarzania przez Procesora, zgodnie z zasadami określonymi w niniejszym ust. 7. Procesor zobowiązany jest do poinformowania Administratora o zamiarze powierzenia innemu podmiotowi przetwarzającemu Danych osobowych do przetwarzania, a także o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia podmiotów przetwarzających Dane osobowe w celu uzyskania uprzedniej pisemnej zgody lub wyrażenia sprzeciwu przez Administratora na dokonanie takiego powierzenia lub dokonanie ww. zmian. Procesor jest zobowiązany do przekazania w formie pisemnej Administratorowi wszelkich niezbędnych informacji dotyczących innego podmiotu przetwarzającego w zakresie spełniania przez niego wymogów niniejszej Umowy oraz przepisów prawa, w tym RODO, w tym w szczególności opisu wdrożonych przez ten podmiot mechanizmów zabezpieczających bezpieczeństwo przetwarzania danych osobowych. Procesor jest uprawniony do zawarcia umowy z ww. innym podmiotem przetwarzającym, o którym Procesor w ww. sposób powiadomił Administratora, wyłącznie w przypadku gdy Administrator wyraził pisemną zgodę lub nie wyraził sprzeciwu w terminie 40 dni roboczych od dnia wpłynięcia do Administratora pisemnej informacji o zamiarze powierzenia przez Procesora Danych osobowych.
17. Procesor zobowiązuje się do niezwłocznego, jednak nie później niż w ciągu 7 dni od powzięcia takiej informacji, poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym Przetwarzania Danych osobowych przez Procesora, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym Przetwarzania Danych osobowych, skierowanej do Procesora, a także o wszelkich kontrolach i inspekcjach dotyczących Przetwarzania Danych osobowych przez Procesora prowadzonych przez organ nadzorczy w zakresie Danych osobowych.
18. W przypadku rozwiązania Umowy lub Umowy głównej Procesor zobowiązany jest, zależnie od decyzji Administratora, do usunięcia lub zwrócenia Administratorowi wszelkich Danych osobowych oraz do usunięcia wszelkich ich istniejących kopii i potwierdzenia tego faktu odpowiednim protokołem, który zostanie przekazany Administratorowi nie później niż w terminie 14 dni od dnia rozwiązania Umowy lub Umowy głównej chyba, że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie Danych osobowych.
19. Planując dokonanie zmian w sposobie Przetwarzania Danych osobowych, Procesor ma obowiązek zastosować się do wymogów, o których mowa w art. 25 ust. 1 RODO i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Procesora zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa Danych osobowych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek Przetwarzania Danych osobowych przez Procesora.

**§ 5**

**Prawo kontroli**

1. Administrator zgodnie z art. 28 ust. 3 pkt h) RODO ma prawo kontroli, czy środki zastosowane przez Procesora przy Przetwarzaniu Danych osobowych i zabezpieczeniu powierzonych Danych osobowych spełniają postanowienia Umowy.
2. Procesor zobowiązany jest umożliwiać Administratorowi, lub wskazanej przez Administratora osobie trzeciej, dokonanie audytów lub inspekcji, aby potwierdzić, iż przetwarzanie przebiegło zgodnie z prawem oraz niniejszą Umową, a także wykonać wynikające z nich zalecenia, aby zapewnić zgodne z prawem Przetwarzanie Danych osobowych powierzonych Procesorowi.
3. Administrator realizować będzie prawo audytu lub inspekcji w godzinach pracy Procesora.
4. Procesor zobowiązuje się do usunięcia uchybień stwierdzonych podczas audytu lub inspekcji w terminie wskazanym przez Administratora.
5. Procesor udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

**§ 6**

**Odpowiedzialność stron**

1. Procesor jest odpowiedzialny za udostępnienie lub wykorzystanie Danych osobowych niezgodnie z przepisami prawa, w tym RODO, lub treścią Umowy, a w szczególności za udostępnienie powierzonych do Przetwarzania Danych osobowych osobom nieupoważnionym.
2. Procesor odpowiada za szkody spowodowane zastosowaniem lub nie zastosowaniem właściwych środków bezpieczeństwa.
3. Procesor odpowiada za szkody, jakie powstaną u Administratora lub osób trzecich w wyniku niezgodnego z RODO lub niniejszą Umową Przetwarzaniem Danych osobowych przez Procesora.
4. W przypadku niewykonania lub nienależytego wykonania przez Procesora niniejszej Umowy, Procesor zobowiązuje się do zapłaty odszkodowania na zasadach ogólnych, z zastrzeżeniem pierwszeństwa zasad odpowiedzialności określonych w Umowie głównej, w szczególności w § 17 ust. 2 lit. j. Umowy głównej.
5. Procesor ponosi odpowiedzialność za działania i zaniechania podmiotów, którym powierza Przetwarzanie Danych osobowych, jak za swoje własne działania i zaniechania, w tym w szczególności zasady określone niniejszym § 6 stosuje się wobec Procesora w przypadku, gdy wskazane w § 6 okoliczności spowodowane zostały przez ww. podmioty, którym Procesor powierzył Dane osobowe do Przetwarzania.

**§ 7**

**Wynagrodzenie**

Wykonanie przedmiotu niniejszej Umowy przez Procesora objęte jest wynagrodzeniem z tytułu wykonania Umowy głównej i nie będzie wiązać się z dodatkowymi kosztami dla Administratora, ponad koszty przewidziane w Umowie głównej.

**§ 8**

**Zasady zachowania poufności**

1. Procesor zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i Danych osobowych otrzymanych od Administratora i od współpracujących z nimi osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („Dane poufne”).
2. Procesor oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy Danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy. Procesor jest zobowiązany do zachowania poufności Danych poufnych przez okres obowiązywania niniejszej Umowy, jak również po jej rozwiązaniu lub wygaśnięciu.

**§ 9**

**Osoby do kontaktu w zakresie Przetwarzania Danych osobowych**

1. Dane kontaktowe inspektora danych osobowych - Administratora: [daneosobowe@metropoliagzm.pl](mailto:daneosobowe@metropoliagzm.pl). Pozostałe aktualne dane dostępne są na stronie bip.metropoliagzm.pl
2. Dane kontaktowe *<inspektora danych osobowych* Procesora */ osoby wyznaczonej do kontaktu w sprawie przetwarzania danych osobowych: ………………………………..>*

**§ 10**

**Postanowienia końcowe**

1. Niniejsza Umowa wchodzi w życie z dniem jej podpisania i zostaje zawarta na czas obowiązywania Umowy głównej oraz wykonania wszystkich zobowiązań wynikających z niniejszej Umowy.
2. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Procesor:
3. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
4. przetwarza Dane osobowe w sposób niezgodny z Umową;
5. powierzył Przetwarzanie Danych osobowych innemu podmiotowi bez zgody Administratora lub pomimo wyrażenia sprzeciwu przez Administratora.
6. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności, z zastrzeżeniem zdania następnego. Nie stanowi zmiany niniejszej Umowy zmiana danych określonych w § 9 niniejszej Umowy, dla której skuteczności wystarczające jest zawiadomienie drugiej Strony pisemnie lub za pośrednictwem wiadomości mailowej, skierowanej na adres mailowy Kierownika Projektu drugiej Strony, określonego na podstawie Umowy głównej, wraz z jednoczesnym powiadomieniem o nowych danych kontaktowych.
7. W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy a Umowy głównej, w zakresie dotyczącym Przetwarzania Danych osobowych, pierwszeństwo mają postanowienia niniejszej Umowy, z zastrzeżeniem § 6 ust. 4 *in fine* niniejszej Umowy. Oznacza to także, że kwestie dotyczące Przetwarzania Danych osobowych pomiędzy Administratorem a Procesorem należy regulować poprzez zmiany niniejszej Umowy.
8. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy RODO oraz Kodeksu cywilnego.
9. Spory związane z wykonywaniem niniejszej Umowy rozstrzygane będą przez sąd właściwy dla siedziby Administratora.
10. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach – jeden dla Procesora, zaś dwa – dla Administratora.

………………………………….. …..……………………………

Administrator Procesor

**Załącznik nr 1**

**Opis wdrożonych mechanizmów zapewniających bezpieczeństwo Przetwarzania Danych osobowych**

Administrator wymaga aby Procesor stosował/ wdrożył następujące mechanizmy zapewniające bezpieczeństwo przetwarzania danych osobowych:

1. System zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu przetwarzającego warunków umożliwiających realizację i egzekwowanie następujących działań:
   1. zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,
   2. utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację,
   3. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,
   4. 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,
   5. zapewnienie szkoleń 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. przetwarzanie danych osobowych,
      4. privacy by default i privacy by design.
      5. stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.
   6. 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. zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.
   7. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
   8. zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
   9. zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
   10. ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
   11. zapewnienie odpowiedniego poziomu bezpieczeństwa systemów 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. kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.
   12. zapewnienie zasad identyfikacji zdarzeń bezpieczeństwa, ich klasyfikacji i bezzwłocznego zgłaszania, w szczególności zdarzeń, których skutkiem jest naruszenie bezpieczeństwa informacji, umożliwiający szybkie podjęcie działań korygujących,
   13. zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
3. Wymagania określone w pkt 1 i 2 uznaje się za spełnione w szczególności, jeżeli stosowany system zarządzania bezpieczeństwem informacji został opracowany na podstawie normy ISO/IEC 27001:2005 w zakresie:
   1. Polityka bezpieczeństwa,
   2. organizacja bezpieczeństwa informacji,
   3. zarządzanie aktywami,
   4. bezpieczeństwo [zasobów ludzkich](https://pl.wikipedia.org/wiki/Zasoby_ludzkie),
   5. bezpieczeństwo fizyczne i środowiskowe,
   6. zarządzanie systemami i sieciami,
   7. kontrola dostępu,
   8. zarządzanie ciągłością działania,
   9. pozyskiwanie, rozwój i utrzymanie systemów informatycznych,
   10. zarządzanie incydentami związanymi z bezpieczeństwem informacji,
   11. zgodność z wymaganiami prawnymi i własnymi standardami,

a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie norm związanych z tą normą, w tym:

1. ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;
2. ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;
3. ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.
4. W przypadku, gdy w trakcie obowiązywania niniejszej Umowy którakolwiek z norm określonych w punkcie 3 powyżej ulegnie zdezaktualizowaniu lub zastąpieniu, Procesor zobowiązuje się stosować normę zaktualizowaną lub zastępującą ww. normę w taki sposób, aby zapewnić w sposób ciągły i niezakłócony pełne bezpieczeństwo powierzonych mu do Przetwarzania Danych osobowych zgodnie z zasadami określonymi w niniejszej Umowie.

**Załącznik nr 2**

**Zakres powierzonych do przetwarzania Danych osobowych**

|  |  |  |
| --- | --- | --- |
| Kategoria osób, których dane dotyczą | Kategorie danych osobowych | Operacje wykonywane na danych |
| [do uzupełnienia przez Administratora przed podpisaniem umowy] | [do uzupełnienia przez Administratora przed podpisaniem umowy] | [do uzupełnienia przez Administratora przed podpisaniem umowy] |
| [do uzupełnienia przez Administratora przed podpisaniem umowy] | [do uzupełnienia przez Administratora przed podpisaniem umowy] | [do uzupełnienia przez Administratora przed podpisaniem umowy] |
| [do uzupełnienia przez Administratora przed podpisaniem umowy] | [do uzupełnienia przez Administratora przed podpisaniem umowy] | [do uzupełnienia przez Administratora przed podpisaniem umowy] |