POLITYKA PRYWATNOŚCI
w zakresie ochrony danych osobowych w Grupie Kapitałowej LV Development

Rozdział I. Postanowienia ogólne

§ 1

1. Grupę Kapitałową LV Development tworzą następujące podmioty: LV Development Sp. z o.o. z siedzibą w Zalesiu (KRS: 0000372979), LV Development Nieruchomości Sp. z o.o. z siedzibą w Krakowie (KRS: 0000895118), LV Development Inwestycje Sp. z o.o. z siedzibą w Zalesiu (KRS: 0000989635) oraz LV Development Chorzów Sp. z o.o., z siedzibą w Krakowie (KRS: 0001071025) LV DEVELOPMENT CONSTRUCTION SP. Z O. O. (KRS: 0000980234) – dalej jako: „**Grupa Kapitałowa**".
2. Administratorem głównym danych osobowych Grupy Kapitałowej jest LV Development Nieruchomości Sp. z o.o. z siedzibą w Krakowie, adres: ul. Przewóz 34D/5, 30-716 Kraków, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie, XI Wydział Gospodarczy KRS pod numerem: 0000895118, o numerze NIP: 6751749322 oraz REGON: 388707210 – dalej jako: „**Administrator**".
3. Podmioty tworzące Grupę Kapitałową LV Development zawarły umowę o współadministrowanie danych osobowych, której celem jest zagwarantowanie klientom i kontrahentom Grupy przetwarzanie danych osobowych na możliwie najwyższym poziomie prywatności .
4. Ustala się niniejszym następujące wytyczne polityki prywatności danych osobowych w Grupie Kapitałowej LV DEverlopment, zwane dalej „Polityką prywatności ".

§ 2

1. Przetwarzanie danych osobowych w Grupie Kapitałowej LV Development jest dopuszczalne pod warunkiem przestrzegania przepisów:
   1) 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 praz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenia o ochronie danych) – dalej RODO;
   2) przepisów innych ustaw, a także rozporządzeń normujących problematykę przetwarzania danych osobowych;
   3) wewnętrznych aktów normatywnych Administratora (uchwał Senatu ADMINISTRATOR i zarządzeń Rektora) regulujących sprawy dotyczące ochrony danych osobowych.
2. Administrator przetwarza dane osobowe w celu:
   1) zapewnienia prawidłowej, zgodnej z prawem polityki personalnej w związku z obsługą procesów prowadzonych przez członków Grupy Kapitałowej, w szczególności prawidłowej realizacji procesu inwestycyjnego, prawidłowej i bezpiecznej obsługi transakcji rezerwacji oraz nabycia lokali oraz innych towarów i usług oferowanych przez członków Grupy Kapitałowej na rzecz klientów i kontrahentów,
   2) dla celów marketingowych związanych z działalnością spółek tworzących Grupę Kapitałową,
   3) dla wypełnienia obowiązków prawnych ciążących na administratorze, jako pracodawcy,
   4) dla realizacji innych celów i zadań – w szczególności wynikających z przepisów prawa lub prawnie uzasadnionych interesów Administratora,
   5) w pozostałych, prawnie uzasadnionych celach – za zgodą osób, których dane dotyczą.

§ 3

1. Polityka prywatności w zakresie ochrony danych osobowych, uwzględniając zasady wynikające z art. 5 RODO zapewnia, aby dane te były:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada zgodności z prawem, rzetelności i przejrzystości);

2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów historycznych lub statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami (zasada ograniczenia celu, celowości);

3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych);

4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (zasada prawidłowości);

5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą (zasada ograniczenia przechowywania);

6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (zasada integralności i poufności);

7) przetwarzane w sposób, który pozwoli administratorowi wykazać, iż spełnione są zasady wymienione w pkt 1-6 (zasada rozliczalności).

2. Szczególnej ochronie podlegają dane osobowe wymienione w art. 9 ust. 1 RODO, tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej, a także dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków prywatności – art. 10 RODO.

§ 4

1. Polityka prywatności w zakresie ochrony danych osobowych odnosi się do danych osobowych przetwarzanych w:

   1) zbiorach danych tradycyjnych, na papierowych nośnikach danych (dokumentacja papierowa, np. kartoteki, księgi, wykazy, listy itp.),

   2) systemach informatycznych i na nośnikach cyfrowych,

   3) systemach dozoru wizyjnego (monitoring).

2. Polityka prywatności w zakresie ochrony danych osobowych realizowana jest w Grupie Kapitałowej przez wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, w szczególności przez osoby odpowiedzialne za nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z przepisów prawa oraz uregulowań wewnętrznych w tym zakresie.
3. Polityka prywatności obowiązuje we wszystkich obiektach, lokalizacjach, komórkach organizacyjnych i stanowiskach pracowniczych Administratora. Odnosi się do wszystkich chronionych danych osobowych przetwarzanych u Administratora, niezależnie od formy, celu oraz zakresu ich przetwarzania (tradycyjnego i elektronicznego).
4. Procedury i zasady określone w Polityce prywatności mają zastosowanie do wszystkich osób wykonujących prace związane z działalnością Administratora lub na rzecz Administratora (niezależnie od formy współpracy, czy rodzaju umowy) w szczególności pracowników, współpracowników (w tym zleceniobiorców i osób realizujących umowy o dzieło) oraz innych osób, którym zostało udzielone upoważnienie do przetwarzania danych osobowych.
5. Administrator, jego pracownicy i współpracownicy deklarują pełne zaangażowanie dla prywatności przetwarzania danych osobowych przetwarzanych zarówno w sposób tradycyjny, jak i w systemach informatycznych oraz na nośnikach cyfrowych.

§ 5

Administrator stosuje środki organizacyjne i techniczne, w tym informatyczne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, w szczególności wprowadza rozwiązania dotyczące:

1) pseudonimizacji i szyfrowania danych osobowych,

2) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych,

3) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, skutkującego naruszeniem ochrony danych osobowych,

4) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

§ 6

Dokumentacja dotycząca sposobu przetwarzania danych oraz środki ochrony danych osobowych powstają w oparciu o:

1) przepisy prawa powszechnie obowiązującego,

2) niniejszą Politykę prywatności w zakresie ochrony danych osobowych,

Rozdział II.
Zasady udostępniania danych osobowych oraz prawa osób, których dane osobowe są przetwarzane przez Administratora

§ 7

1. Administrator udostępnia przetwarzane w swoich zasobach dane osobowe wyłącznie:
   1) osobom, które przetwarzają dane osobowe na polecenie Administratora tj. posiadającym upoważnienie do przetwarzania danych osobowych – co do zbioru i zakresu. Wszystkie osoby, którym zostaje udzielone upoważnienie do przetwarzania danych osobowych są zobowiązane do podpisania oświadczenia o zachowaniu poufności danych osobowych – wzór oświadczenia stanowi Załącznik nr 1 do niniejszej Polityki.
   2) podmiotom przetwarzającym, tj. osobom lub podmiotom, których charakter pracy wymaga udostępnienia im takich danych – na podstawie umowy powierzenia przetwarzania danych osobowych, która w szczególności określa:
   a) przedmiot i czas trwania przetwarzania
   b) charakter i cel przetwarzania
   c) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą
   d) obowiązki podmiotu przetwarzającego wynikające z art. 28 RODO.
   3) podmiotom kontrolnym uprawnionym do kontroli działalności Administratora oraz podmiotom uprawnionym do przetwarzania danych osobowych – na podstawie przepisów prawa.
2. Dostęp do danych osobowych, o którym mowa w ust. 1 pkt 3, po okazaniu dokumentów potwierdzających uprawnienia mogą mieć w szczególności pracownicy: Państwowej Inspekcji Pracy, Zakładu Ubezpieczeń Społecznych, organów kontroli skarbowej, Policji i służb specjalnych (Agencji Prywatności Wewnętrznego, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego), sądów powszechnych, Najwyższej Izby Kontroli, Urzędu Ochrony Danych Osobowych, a także inne osoby, podmioty i organy upoważnione przez przepisy prawa i działające w granicach przyznanych im uprawnień.

§ 8

1. Osoba, której dane osobowe dotyczą, na podstawie art. 15 RODO ma prawo do uzyskania potwierdzenia, czy jej dane osobowe są przetwarzane w Administratora, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji o: 1) celu przetwarzania; 2) kategorii odnośnych danych osobowych; 3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych; 4)

w miarę możliwości - planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu; 5) prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz prawie do wniesienia sprzeciwu wobec takiego przetwarzania; 6) prawie wniesienia skargi do organu nadzorczego; 7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle; 8) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, RODO oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Administrator w ramach wypełnienia tzw. obowiązku informacyjnego określonego w art. 13 i 14 RODO podaje informacje wskazane w ust.1 w stosownych klauzulach informacyjnych. Klauzule informacyjne są dostępne na serwisie internetowym Administratora oraz są przekazywane odpowiednim adresatom wraz z dokumentacją papierową.
3. W przypadkach i na zasadach określonych w art. 16-22 RODO, osoba, której dane osobowe dotyczą ma prawo do: 1) żądania, aby jej dane osobowe zostały niezwłocznie sprostowane, jeżeli są nieprawidłowe lub aby zostały uzupełnione, jeżeli dane te są niekompletne, 2) żądania usunięcia danych osobowych, 3) żądania ograniczenia przetwarzania danych osobowych, 4) otrzymania w określonym formacie danych osobowych i przesłania ich do innego administratora lub żądania przesłania takich danych bezpośrednio innemu administratorowi, 5) wniesienia sprzeciwu – z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania jej danych osobowych, 6) niepodlegania decyzji podjętej wyłącznie na podstawie przetwarzania, które odbywa się w sposób zautomatyzowany (np. profilowanie)

Rozdział III.
Obszary przetwarzania danych osobowych oraz zastosowane w nich środki techniczne i organizacyjne zapewniające przetwarzanie danych zgodnie z RODO

§ 9

1. Za fizyczny obszar przetwarzania danych osobowych przez Administratora uważa się wszystkie budynki, pomieszczenia lub części pomieszczeń, w których przetwarzane są dane osobowe na nośnikach papierowych. W szczególności jest to obszar bieżącego przechowywania dokumentów oraz obsługi osób, których dane dotyczą. Za wirtualny obszar przetwarzania danych osobowych przez Administratora uważa się miejsce, w którym znajduje się urządzenie umożliwiające dostęp do danych osobowych przetwarzanych w systemie informatycznym. Za szczególny wirtualny obszar przetwarzania danych osobowych uważa się tzw. chmurę, czyli usługę internetową umożliwiającą tworzenie, udostępnianie, przesyłanie i przechowywanie plików (dokumentów, zdjęć, plików multimedialnych itp.) oraz komunikowanie się i pracę grupową w formie online, z użyciem serwerów niebędących własnością Administratora, których wydzielona część udostępniona jest w ramach wykupionej licencji (np. wirtualny dysk OneDrive, usługa SharePoint, przestrzeń dyskowa przydzielana dla zespołów w Microsoft Teams, platforma Zoom itp.).

§ 10

1. W obszarze fizycznym przetwarzania danych osobowych przez Administratora zastosowane są rozwiązania uniemożliwiające dostęp osób nieuprawnionych oraz zapobiegające wystąpieniu przypadkowych zdarzeń o charakterze siły wyższej. W szczególności są to zabezpieczenia fizyczne, takie jak: 1) wzmocnione drzwi, 2) pomieszczenia zamykane na klucz, 3) elektroniczne systemy alarmowe, 4) zamykane na klucz meble biurowe, 5) zabezpieczenie okien, 6) alarm przeciwpożarowy, 7) system dozoru wizyjnego z użyciem kamer, 8) alarm antywłamaniowy.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe podlega nadzorowi i kontroli.

§ 11

1. W obszarze wirtualnym przetwarzania danych osobowych przez Administratora zastosowane są rozwiązania uniemożliwiające dostęp osób nieuprawnionych oraz zapobiegające wystąpieniu

przypadkowych zdarzeń o charakterze siły wyższej. W szczególności są to zabezpieczenia techniczne/informatyczne, takie jak: 1) dostęp do systemu informatycznego poprzez logowanie, 2) wymóg stosowania haseł o odpowiednio wysokim stopniu skomplikowania, 3) tworzenie kopii zapasowych baz danych zawierających dane osobowe, 4) ograniczenie ruchu dla usług publicznych, 5) stosowanie zapory ogniowej (firewall) oraz jej bieżący monitoring, 6) stosowanie ochrony antywirusowej, antyszpiegowskiej i antyreklamowej, 7) bieżąca aktualizacja oprogramowania, 8) weryfikacja podmiotów świadczących usługi hostingu lub dostawców usług SaaS (Software as a Service), 9) zezwolenie na przetwarzanie danych osobowych stanowiących zasoby Administratora przy użyciu komputerów przenośnych – wyłącznie w przypadkach, gdy komputery takie stanowią wyposażenie pracowników (sprzęt służbowy) i są odpowiednio zabezpieczone (zaszyfrowane); 10) zezwolenie na przetwarzanie, w szczególności przechowywanie danych osobowych stanowiących zasoby Administratora na nośnikach cyfrowych (dysk przenośny, pendrive itp.) – wyłącznie w przypadkach, gdy nośniki takie stanowią wyposażenia pracowników (sprzęt służbowy) i są odpowiednio zabezpieczone (zaszyfrowane); 11) zakaz przetwarzania danych osobowych, które nie stanowią zasobów Administratora (dane prywatne) na służbowym sprzęcie.

2. Pod szczególną ochroną pozostają urządzenia stanowiące zasoby sprzętowe systemu informatycznego – stacje robocze pracowników przetwarzających dane osobowe wchodzące w skład tego systemu powinny być umiejscowione w taki sposób, aby uniemożliwić dostęp osobom nieuprawnionym (w szczególności dostęp do monitorów oraz urządzeń służących do kopiowania danych).

Rozdział VI.
Zasady prywatności zapewniające przetwarzanie danych zgodnie z RODO

§ 12

1. U Administratora stosowane są następujące zasady bezpiecznego przetwarzania danych osobowych:
   1) zakaz udostępniania haseł dostępu do systemów informatycznych lub pozostawiania ich w łatwo dostępnych miejscach na stanowisku pracy,
   2) zakaz udzielania informacji zawierających dane osobowe w rozmowach przez telefon, z osobami, których tożsamości nie można jednoznacznie zweryfikować i potwierdzić,
   3) wymóg zachowania podwyższonej ostrożności wobec wiadomości e-mail otrzymanych od niezweryfikowanych nadawców – zakaz klikania w podejrzane linki i otwierania nieznanych załączników,
   4) wymóg stosowania szyfrowania załączników zawierających dane osobowe, wysyłanych e-mailem poza obszar domeny Administratora,
   5) wymóg pracy w odpowiednim skupieniu i bez nadmiernego pośpiechu,
   6) podczas opuszczania systemu informatycznego - wymóg wyrobienia nawyku wylogowania poprzez przycisk,
   7) po zakończeniu pracy – wymóg bieżącego usuwania zbędnych danych, zarówno w odniesieniu do dokumentów papierowych, jak i w wersji elektronicznej.
2. Podczas pracy w każdym systemie informatycznym stosowane są następujące zasady ogólne:
   1) dane osobowe w systemach informatycznych może przetwarzać wyłącznie osoba posiadająca pisemne upoważnienie administratora. Pracownicy/współpracownicy mają dostęp wyłącznie do danych w takim zakresie, jaki został wskazany w upoważnieniu i wynika z umowy o pracę lub umowy cywilnoprawnej oraz przydzielonych zadań/obowiązków (zasada wiedzy koniecznej i zasada minimalizacji danych);
   2) użytkownik systemu informatycznego jest zobowiązany do logowania się w taki sposób, aby uniemożliwić poznanie loginu i hasła przez osoby nieupoważnione.

§ 13

1. Czasowe (w trakcie pracy) opuszczenie przez pracownika stanowiska, na którym przetwarzane są dane osobowe, wiąże się z zastosowaniem dostępnych środków zabezpieczających, by chronić używane zasoby danych osobowych przed dostępem do nich osób nieuprawnionych.

2. Całkowite (po zakończeniu pracy w danym dniu) opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, wiąże się z zastosowaniem wszystkich dostępnych środków zabezpieczających to pomieszczenie przed wejściem tam osób niepowołanych.
3. Zabronione jest opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zastosowania odpowiedniego zabezpieczenia. Wszelkie konsekwencje takiego naruszenia mogą być traktowane jako niedopełnienie podstawowych obowiązków pracowniczych.

Rozdział V.
Zasady przetwarzania danych osobowych w zbiorach
§ 14

1. Przetwarzane przez Administratora dane osobowe są gromadzone w zbiorach, tworzonych w taki sposób, aby odpowiednie dane były dostępne w oparciu o określone kryteria, niezależnie od tego, czy zestaw danych jest scentralizowany lub zdecentralizowany albo rozproszony funkcjonalnie lub geograficznie.
2. Podstawowymi zbiorami danych tworzonymi u Administratora są dane osobowe: klientów, kandydatów do pracy, pracowników, emerytów i członków rodzin pracowników, kontrahentów (w tym zleceniobiorców i zleceniodawców), interesariuszy, stron oraz innych osób fizycznych, których dane osobowe Administrator jest uprawniony przetwarzać na podstawie przepisów prawa lub na podstawie zgody wyrażonej przez osoby, których dane dotyczą.
3. U Administratora mogą być tworzone również inne zbiory danych, w celach doraźnych, ze względów technicznych lub w związku z realizacją określonego zadania. Zbiory te, po ich wykorzystaniu są niezwłocznie usuwane albo poddane modyfikacji tak, by danych w nich zawartych nie można było przypisać konkretnej lub dającej się ustalić osobie (anonimizacja) lub aby konieczny był w tym celu nieproporcjonalnie duży nakład czasu, kosztów i pracy (pseudonimizacja lub szyfrowanie).
4. Administrator sprawuje nadzór nad wszelkimi zbiorami danych osobowych tworzonymi na jej obszarze. Zabronione jest przetwarzanie danych osobowych, w tym tworzenie zbiorów danych, a także gromadzenie w zbiorach lub poza nimi danych osobowych - innych niż niezbędne dla realizacji celów, do których dane te zostały zebrane. Wszelkie nowe programy i systemy informatyczne, które mają służyć gromadzeniu i przetwarzaniu danych osobowych u Administratora muszą zapewniać możliwość obsługi określonych zbiorów danych oraz spełniać wymogi prywatności wskazane przez Administratora.

Rozdział VI.
Postanowienia końcowe
§ 15

1. Administrator na bieżąco dokłada wszelkich starań, aby gromadzone i przetwarzane dane osobowe podlegały ochronie zgodnie z wymogami obowiązującego w tym zakresie prawa.
2. Mając na uwadze stałe podnoszenie poziomu prywatności przetwarzania danych osobowych, Administrator na bieżąco wdraża środki techniczne (w tym informatyczne) i organizacyjne, które pozwalają minimalizować ryzyko związane z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Administrator stosuje środki organizacyjne zapewniające utrzymanie poufności, integralności i rozliczalności przetwarzanych danych osobowych, w szczególności: 1) prowadzona jest ewidencja osób, którym nadano upoważnienie do przetwarzania danych osobowych; 2) promowana jest ogólna zasada poufności danych osobowych – w każdym aspekcie funkcjonowania Administratora; 3) prowadzone są szkolenia wewnętrzne i wydawane są instrukcje oraz zalecenia podnoszące świadomość pracowników w zakresie prywatności przetwarzania danych osobowych; 4) prowadzona jest ocena ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, w związku z przetwarzaniem danych osobowych; 5) dokonywana jest ocena skutków dla ochrony danych osobowych w odniesieniu do planowanych operacji przetwarzania, w szczególności z użyciem nowych technologii – w przypadku, gdy zostanie stwierdzone, że dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

§16

1. Niniejsza polityka prywatności jest na bieżąco poddawana analizie i w razie potrzeby aktualizowana. Wraz z przeglądem Polityki prywatności Administrator kontroluje również pracowników i inne podmioty upoważnione do przetwarzania danych osobowych pod kątem przestrzegania przez te osoby niniejszej Polityki oraz przepisów RODO (audyty doraźne).
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie potwierdzające znajomość jego treści.
3. Załączniki: Zał. 1 – wzór oświadczenia o zachowaniu poufności.

Załącznik nr 1 do Polityki prywatności w zakresie ochrony danych osobowych

(imię i nazwisko) ……

(stanowisko) ……

Oświadczenie osoby posiadającej dostęp do danych osobowych

Ja niżej podpisana/-y, zobowiązuję się do zachowania poufności danych osobowych, do których przetwarzania zostało mi wydane upoważnienie w związku z wykonywaniem przeze mnie obowiązków w ramach spółek tworzących Grupę Kapitałową LV Development.

Zobowiązuję się do przestrzegania wszelkich przepisów prawa dotyczących ochrony danych osobowych.

Potwierdzam, że jest mi znana definicja danych osobowych w rozumieniu art. 4 pkt 1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 roku oraz, że zapoznałam/-em się z przepisami dotyczącymi ochrony danych osobowych.

Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie obowiązków pracowniczych w rozumieniu Kodeksu pracy oraz może być podstawą do realizacji uprawnień przez Administratora.

Znam zakres odpowiedzialności karnej określony w Ustawie z dnia 10 maja 2018 roku o ochronie danych osobowych i Ustawie z dnia 6 czerwca 1997 r. Kodeks karny.

……..

(data i podpis osoby składającej oświadczenie)