Polityka Ochrony Danych osobowych
w Centrum Finansowo-Księgowym EKKOM Sp. z o.o.
oraz spółkach powiązanych
z dnia 25 maja 2018 r.

Uwzględniając obowiązki wynikające z art. 25 oraz art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1), celem zapewnienia, że dane osobowe w Spółce **Centrum Finansowo-Księgowe EKKOM Sp. z o.o.** i spółkach powiązanych są przetwarzane i zabezpieczone zgodnie z postanowieniami prawa poprzez wdrożenia odpowiednich środków technicznych i organizacyjnych zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń; oraz zapewnia, że domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

§ 1 Postanowienia wstępne

1.1. Polityka określa zasady przetwarzania oraz zabezpieczania Danych osobowych w Spółce, celem zapewnienia zbieżności Przetwarzania z wymaganiami RODO oraz przepisami bezwzględnie obowiązującego prawa polskiego w zakresie przetwarzania danych osobowych. Polityka stanowi zbiór oraz podstawę wdrażanych w Spółce wymogów, procedur oraz zasad ochrony danych osobowych. Polityka zawiera:

(i) opis zasad ochrony danych obowiązujących w Spółce;

(ii) zbiór procedur, instrukcji i regulacji szczegółowych dotyczących przetwarzania Danych osobowych w Spółce, dotyczących poszczególnych obszarów z zakresu ochrony danych osobowych; stanowiących załączniki do Polityki.

1.2. Polityka obowiązuje wszystkich pracowników oraz współpracowników Spółki. Polityka obowiązuje również wszystkie podmioty powiązane kapitałowo lub osobowo ze Spółką. Listę podmiotów powiązanych zawiera **Załącznik nr 1**. Za przestrzeganie i utrzymanie postanowień Polityki odpowiedzialni są:

(i) Spółka;

(ii) komórki organizacyjne Spółki, w których przetwarzane są Dane osobowe;

(iii) Pracownicy.

1.3. Pracownicy oraz współpracownicy Spółki oraz spółek powiązanych, oddelegowani do pracy u klienta Spółki, zobowiązani są w pierwszej kolejności do przestrzegania Polityki bezpieczeństwa funkcjonującej u klienta, a dopiero później do przestrzegania postanowień niniejszej Polityki.

1.4. Dla skutecznej realizacji Polityki, uwzględniając zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia Spółka zapewnia:

(i) wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania Danych osobowych z wymogami prawa oraz niezbędne zabezpieczenie przetwarzanych danych osobowych;

(ii) stałe monitorowanie zgodności przetwarzania Danych osobowych z wymogami prawa oraz poddawanie środków, o których mowa w ust. 1.4.(i) wyżej ciągłym przeglądom oraz uaktualnianiu;

(iii) kontrolę i nadzór nad przetwarzaniem Danych osobowych.

1.5. Nadzór nad przestrzeganiem postanowień polityki zapewnia Zarząd Spółki. Nadzór, o którym mowa w zdaniu poprzedzającym zmierza w szczególności, ale nie wyłącznie do zapewnienia, że czynności związane z przetwarzaniem Danych osobowych w Spółce są zgodne z wymogami prawa oraz postanowieniami Polityki.

1.6. Spółka zapewnia zgodność postępowania kontrahentów Spółki, w tym w szczególności Podmiotów Przetwarzających i Podmiotów Współprzetwarzających z postanowieniami Polityki w odpowiednim zakresie we wszystkich sytuacjach, w których dochodzi do przekazania tym podmiotom Danych osobowych do przetwarzania, w tym przechowywania.

1.7. Polityka jest przechowywana i udostępniana w wersji papierowej oraz elektronicznej w siedzibie Spółki.

1.8. Politykę udostępnia się:

(i) obligatoryjnie wszystkim osobom upoważnionym do przetwarzania danych osobowych w Spółce, celem zapewnienia osobom upoważnionym należytej wiedzy oraz informacji na temat zasad i wymogów dotyczących przetwarzania Danych Osobowych w Spółce;

(ii) osobom zainteresowanym, w szczególności osobom fizycznym, których dane dotyczą – na ich wniosek.

§ 2 Słownik pojęć

2.1. Ilekroć w niniejszej Polityce zostaną wykorzystane poniższe definicje lub zwroty, należy nadawać im następujące znaczenie:

(i) Polityka – oznacza niniejszą Politykę wraz ze wszystkimi ewentualnymi Załącznikami;

(ii) Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, takie 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; o których mowa w art. 4 pkt 1 RODO;

(iii) RODO – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1);

(iv) Osoba upoważniona – oznacza osobę upoważnioną przez Spółkę do przetwarzania Danych osobowych w danym zakresie;

(v) Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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, o których mowa w art. 4 pkt 2 RODO;

(vi) Zbiór danych – oznacza każdy uporządkowany zestaw Danych osobowych, dostępny według określonych kryteriów;

(vii) Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Spółki [np. usługodawca IT];

(viii) Podmiot Współprzetwarzający – oznacza osobę fizyczną lub prawną, która przetwarza dane osobowe wspólnie ze spółką na podstawie ścisłego stosunku Współpracy lub powiązań kapitałowych czy osobowych.

(ix) Rejestr - oznacza Rejestr Czynności Przetwarzania Danych Osobowych Spółki;

(x) Uwierzytelnienie – oznacza działanie, którego celem jest weryfikacja deklarowanej tożsamości Użytkownika;

(xi) Spółka – oznacza Centrum Finansowo-Księgowe EKKOM Sp. z o.o., ul. Krotoszyńska 55, 51-009 Wrocław, NIP 8971668503, KRS 0000090054;

(xii) Spółki powiązane – oznacza:

- Centrum Finansowo-Księgowe Ekkom Sp. z o.o. Sp. K., KRS 0000555876;
- Centrum Personalne EKKOM Sp. z o.o., KRS 0000615622;
- Centrum Personalne EKKOM Sp. z o.o. Sp. K., KRS 0000713627;

(xiii) Pracownicy – oznaczają zarówno osoby zatrudnione w Spółce na podstawie stosunku pracy, jak również osoby fizyczne współpracujące ze Spółką na podstawie Umowy cywilnoprawnej;

(xiv) System – oznacza System ochrony danych osobowych w Spółce, o którym mowa w § 5 Polityki;

(xv) Dane wrażliwe – oznaczają Dane Osobowe, o których mowa w art. 9 RODO.

§ 3 Dane osobowe

3.1. Spółka przetwarza Dane osobowe gromadzone w zbiorach danych. Zbiory danych przetwarzane w Spółce określa **Załącznik nr 2** do Polityki.

3.2. Uaktualnienie lub poszerzenie listy Zbiorów danych następuje po uprzednim przeprowadzeniu analizy skutków oraz ryzyk przetwarzania danych osobowych dla praw i wolności osób fizycznych objętych zbiorem.

3.3. Spółka nie podejmuje czynności Przetwarzania, które mogłyby wiązać się z istotnym ryzykiem naruszenia praw i wolności osób, których Dane osobowe dotyczą. W przypadku planowania podjęcia czynności, o których mowa w zdaniu poprzedzającym Spółka

obligatoryjnie przeprowadza uprzednią ocenę skutków przetwarzania, o których mowa w art. 35 RODO.

3.4. Dane osobowe domyślnie Przetwarzane są na obszarze na terenie obejmującym pomieszczenia biurowe Spółki zlokalizowane we Wrocławiu przy ul. Robotniczej 68a. Dodatkowy obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym w zdaniu poprzedzającym.

§ 4 Podstawy ochrony Danych Osobowych w Spółce

4.1. Spółka zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.

4.2. Osoby upoważnione oraz wszystkie inne osoby, którym udostępnia się Dane osobowe Przetwarzane w Spółce zobowiązane są do Przetwarzania Danych osobowych zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych wewnętrznych aktów prawnych Spółki lub procedur wewnętrznych związanych z Przetwarzaniem Danych Osobowych.

4.3. Przy zatrudnianiu Pracowników oraz w toku zatrudnienia Spółka zapewnia, że:

(i) Pracownicy przed przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad Przetwarzania i ochrony Danych Osobowych w Spółki;

(ii) każdy z Pracowników zostaje upoważniony na piśmie do Przetwarzania Danych Osobowych w niezbędnym zakresie, zgodnie z wzorem stanowiącym **Załączniki nr 3** do Polityki;

(iii) każdy z pracowników zostaje zobowiązany do zachowania poufności i integralności Danych osobowych, zgodnie z wzorem stanowiącym **Załącznik nr 4** do Polityki, przy czym Pracownicy zobowiązani są w szczególności, ale nie wyłącznie do:

(a) ścisłego przestrzegania zakresu upoważnienia;

(b) przestrzegania wymogów prawa oraz postanowień Polityki w zakresie przetwarzania;

(c) zachowania w tajemnicy Danych osobowych;

(d) zachowania w tajemnicy sposobów zachowania poufności i integralności Danych Osobowych;

(e) niezwłocznego zgłaszania Spółki wszelkich incydentów związanych z naruszeniem bezpieczeństwa Danych osobowych.

4.4. Spółka zapewnia, aby Dane Osobowe Przetwarzane w Spółce były:

(i) Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;

(ii) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

(iii) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

(iv) 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 ("prawidłowość");

(v) 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;

(vi) 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.

4.5. Przy zapewnieniu Przetwarzania Danych osobowych zgodnie z zasadami wskazanymi w ust. 4.1 wyżej Spółka opiera Przetwarzanie na następujących podstawach:

(i) Legalność – Spółka dba o ochronę prywatności i przetwarza Dane osobowe zgodnie z wymogami prawa;

(ii) Bezpieczeństwo – Spółka zapewnia odpowiedni poziom bezpieczeństwa Danych osobowych podejmując stale działania w tym zakresie;

(iii) Prawa Jednostki – Spółka umożliwia osobom, których Dane Osobowe są przetwarzane, wykonywanie swoich praw i prawa te realizuje;

(iv) Rozliczalność – Spółka zapewnia należyte udokumentowanie sposobu spełniania obowiązków w zakresie ochrony danych osobowych.

4.6. Zgodnie z art. 37 Ustawy z dnia 5 lipca 1996 r. o doradztwie podatkowym (t.j. Dz. U. z 2018 r. poz. 377 ze zm.) Spółka uwzględnia, że Dane osobowe Przetwarzane w związku ze świadczeniem usług doradztwa podatkowego objęte są tajemnicą doradcy podatkowego. W zakresie Przetwarzania Danych osobowych pozyskanych w związku z wykonywaniem czynności objętych tajemnicą doradcy podatkowego Spółka stosuje się do wytycznych oraz wymogów w zakresie zachowania tajemnicy zawodowej.

4.7. Spółka nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej.

§ 5 System ochrony danych osobowych

5.1. Spółka zapewnia zgodność Przetwarzania Danych Osobowych z wymogami prawa również poprzez zaprojektowanie, wprowadzenie i utrzymywanie Systemu. Na System składają się środki organizacyjne oraz środki techniczne ochrony, adekwatne do poziomu ryzyka zidentyfikowanego dla poszczególnych Zbiorów danych oraz kategorii danych. Na System składają się w szczególności następujące środki:

(i) ograniczenie dostępu do pomieszczeń, w których przetwarzane są Dane osobowe, jedynie do Osób upoważnionych oraz zapewnienie, że inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do Przetwarzania Danych osobowych wyłącznie w towarzystwie Osoby upoważnionej;

(ii) zamykanie pomieszczeń tworzących obszar, o którym mowa w ust. 3.4 Polityki na czas nieobecności Pracowników, w sposób uniemożliwiający dostęp do nich osobom trzecim;

(iii) zapewnienie zabezpieczenia obszaru, o którym mowa w ust. 3.4 Polityki przed czynnikami losowymi, takimi jak pożar lub powódź;

(iv) wykorzystywanie zamykanych szafek, szuflad lub innych środków technicznych uniemożliwiających osobom niepowołanym dostęp do przechowywanych w nich Danych osobowych;

(v) wdrożenie Polityki czystego biurka, która stanowi **Załącznik nr 5** do Polityki;

(vi) wdrożenie Procedury otwierania i zamykania budynków oraz pomieszczeń biurowych, która stanowi **Załącznik nr 6** do Polityki;

(vii) zapewnienie skutecznego usuwania lub niszczenia dokumentów zawierających Dane osobowe, w sposób uniemożliwiający ich późniejsze odtworzenie;

(viii) zapewnienie bezpieczeństwa sprzętowego i informatycznego, obejmującego:

(a) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz,

(b) zapewnienie aktualności stosowanego oprogramowania,

(c) zabezpieczenie sprzętu komputerowego wykorzystywanego w Spółce przed złośliwym oprogramowaniem,

(d) zapewnienie stałego i częstotliwego sporządzania kopii zapasowych danych przechowywanych na komputerach, serwerze oraz w sieci Spółki,

(e) ograniczenie dostępu do sprzętu komputerowego, oprogramowania, serwera oraz sieci lokalnej poprzez stosowanie reguł Uwierzytelniania;

(ix) przeprowadzanie analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

(x) realizację standardów weryfikacji i doboru Podmiotów przetwarzających, jak również warunków powierzenia Przetwarzania danych na rzecz poszczególnych Podmiotów przetwarzających;

(xi) monitorowanie zmian w zakresie procesów Przetwarzania Danych osobowych w Spółki oraz na bieżąco zarządza zmianami mającymi wpływ na ochronę Danych osobowych w Spółce.

§ 6 Rejestr

6.1. Rejestr obejmuje kategorie czynności przetwarzania Danych Osobowych w Spółce. Za pośrednictwem Rejestru Spółka dokumentuje czynności przetwarzania Danych Osobowych oraz inwentaryzuje i monitoruje sposób, w jaki wykorzystuje Dane osobowe. Rejestr stanowi **Załącznik nr 7** do Polityki.

6.2. Za pośrednictwem Rejestru, w szczególności poprzez wskazanie w Rejestrze ogólnych środków ochrony Danych Osobowych objętych wyodrębnioną czynnością przetwarzania, Spółka dąży również do wykazania zgodności Przetwarzania Danych Osobowych z wymogami prawa.

6.3. W Rejestrze, odrębnie dla każdej zidentyfikowanej kategorii czynności przetwarzania Danych osobowych, odnotowuje się co najmniej:

(i) nazwę czynności;

(ii) cel przetwarzania;

(iii) opis kategorii osób, których Dane osobowe przetwarzane są w ramach danej czynności;

(iv) opis kategorii Danych osobowych przetwarzanych w ramach danej czynności;

(v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Spółki, jeśli podstawą przetwarzania jest uzasadniony interes;

(vi) opis kategorii odbiorców danych, w tym Podmiotów przetwarzających,

(vii) informację o ewentualnym przekazaniu Danych osobowych poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;

(viii) ogólny opis technicznych i organizacyjnych środków ochrony Danych osobowych, znajdujących zastosowanie do danej czynności.

6.4. W przypadku uaktualnienia lub poszerzenia kategorii czynności przetwarzania Danych Osobowych, Spółka dokonuje niezwłocznego uaktualnienia Rejestru celem zapewnienia zgodności Rejestru ze stanem faktycznym oraz zakresem operacji przetwarzania Danych osobowych w Spółki.

6.5. Postanowienia ust. 6.3 wyżej nie wyłączają możliwości ujęcia w Rejestrze w miarę potrzeby informacji dodatkowych, zwiększających szczegółowość lub czytelność Rejestru lub ułatwiających zarządzanie zgodnością ochrony Danych osobowych z wymogami prawa, oraz realizację zasady rozliczalności.

6.6. Spółka dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania poprzez wskazanie ogólnej podstawy prawnej przetwarzania, takiej jak: zgoda, umowa, obowiązek prawny nałożony na Spółkę, uzasadniony cel Spółki.

§ 7 Realizacja obowiązków wobec osób, których dane osobowe dotyczą

7.1. Spółka wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności, takich jak zgłoszenie sprzeciwu lub ograniczenie przetwarzania.

7.2. Spółka dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których Dane osobowe przetwarza.

7.3. Spółka publikuje na stronie swojej stronie internetowej www.ekkom.com.pl oraz pozostawia do wglądu w siedzibie Spółki:

(i) Politykę;

(ii) Informację o prawach osób, których dane dotyczą;

(iii) Informację o zakresie przetwarzanych danych osobowych w poszczególnych celach;

(iv) Metodach kontaktu ze Spółką w zakresie danych osobowych;

7.4. W celu realizacji praw osoby, której Dane osobowe dotyczą Spółka zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez

Spółkę, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

7.5. Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób, informując osobę, której dane dotyczą:

(i) o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

(ii) o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej;

(iii) o planowanej zmianie celu przetwarzania danych.

(iv) przed uchyleniem ograniczenia przetwarzania.

(v) o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

(vi) o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

7.6. Spółka bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

7.7. Niezależnie od postanowień ust. 7.5 wyżej, Spółka określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

7.8. Na żądanie osoby dotyczące dostępu do jej danych, Spółka informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

7.9. Spółka wydaje osobie, której Dane osobowe dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

7.10. Spółka dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której Dane osobowe dotyczą. Spółka ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.11. Spółka uzupełnia i aktualizuje dane na żądanie osoby, której Dane osobowe dotyczą. Spółka ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Spółka może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Spółkę procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

7.12. Z uwzględnieniem ust. 7.13 niżej, na żądanie osoby, Spółka usuwa dane, gdy:

(i) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

(ii) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

(iii) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

(iv) dane były przetwarzane niezgodnie z prawem,

(v) konieczność usunięcia wynika z obowiązku prawnego,

(vi) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

7.13. Spółka przy usuwaniu danych osobowych uwzględnia, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

7.14. Jeżeli dane podlegające usunięciu zostały upublicznione przez Spółkę, Spółka podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.15. Spółka dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

(i) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

(ii) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

(iii) Spółka nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

(iv) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Spółki zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

7.16. W trakcie ograniczenia przetwarzania Spółka przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.17. Na żądanie osoby Spółka wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Spółce, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Spółki.

7.18. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, o którym mowa w art. 21 RODO, a dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes Spółki lub o powierzone Spółki zadanie w interesie publicznym, Spółka zobowiązuje się uwzględnić sprzeciw, o ile nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

7.19. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Spółkę na potrzeby marketingu bezpośredniego, Spółka uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

§ 8 Minimalizacja danych

8.1. Spółka wdraża procedury służące realizacji zasady minimalizacji przetwarzanych Danych Osobowej pod względem:

(i) adekwatności Danych osobowych do celów Przetwarzania, obejmujących ograniczenie ilości przetwarzanych Danych Osobowych oraz zakresu przetwarzania do celu Przetwarzania;

(ii) ograniczenia dostępu do Danych osobowych wyłącznie do Osób upoważnionych, dla których wykorzystanie Danych osobowych w określonym zakresie jest niezbędne dla prawidłowej realizacji obowiązków;

(iii) ograniczenia czasu przechowywania Danych osobowych do okresu, dla którego przechowywanie Danych osobowych jest niezbędne ze względu na realizację celu Przetwarzania lub obowiązków nałożonych na Spółkę.

8.2. Spółka dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

8.3. Spółka stosuje ograniczenia dostępu do Danych Osobowych poprzez:

(i) zobowiązanie Pracowników do zachowania poufności, w tym w zakresie Danych Osobowych;

(ii) weryfikację kręgu wewnętrznych odbiorców Danych Osobowych poprzez nadawanie poszczególnym Pracownikom szczegółowych upoważnień co do Przetwarzania Danych Osobowych;

(iii) wdrożenie logicznych środków technicznych ochrony Danych osobowych poprzez ograniczenie dostępu do systemów, oprogramowania oraz zasobów sieciowych wykorzystywanych w procesie Przetwarzania Danych Osobowych;

(iv) wdrożenie fizycznych środków technicznych ochrony Danych osobowych, wskazanych w ust. 5.1.(iv) Polityki.

8.4. Spółka dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających. Spółka dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

8.5. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Spółki.

8.6. Spółka przetwarza dane osobowe z uwzględnieniem kryteriów wskazanych w Rejestrze. Spółka wdraża mechanizmy kontroli cyklu życia danych osobowych w Spółce, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

8.7. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów Spółki, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji

przetwarzanych przez Spółkę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

§ 9 Bezpieczeństwo danych osobowych

9.1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia Spółka wdraża środki techniczne i organizacyjne zapewniające należyty stopień ochrony Danych osobowych, odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Spółkę.

9.2. Spółka przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

(i) Spółka kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;

(ii) Spółka przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Spółka analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia;

9.3. Spółka wdraża środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

§ 10 Naruszenie ochrony danych osobowych

10.1. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych Osobowych uważa się w szczególności, ale nie wyłącznie:

(i) Naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są Dane osobowe;

(ii) udostępnienie Danych osobowych osobom nieupoważnionym;

(iii) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich Przetwarzania;

(iv) nieuprawnione lub przypadkowe uszkodzenie, utratę, zniszczenie lub zmianę Danych osobowych.

10.2. W przypadku stwierdzenia naruszenia ochrony danych osobowych Spółka dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych oraz szacuje skalę ryzyka.

10.3. W przypadku naruszenia ochrony Danych Osobowych, Spółka bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Wzór

zawiadomienia, o którym mowa w zdaniu poprzedzającym, stanowi **Załącznik nr 8** do Polityki.

10.4. Jeżeli ryzyko naruszenia praw i wolności osoby, której Dane osobowe dotyczą jest wysokie, Spółka zawiadamia o incydencie także osobę, której dane dotyczą, chyba że:

(i) Spółka wdroży odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, uniemożliwiające osobom nieuprawnionym odczyt oraz dostępu do tych danych osobowych;

(ii) Spółka zastosuje następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; lub

(iii) wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

10.5. Niezależnie od obowiązków wskazanych w ust. 10.2-10.4 wyżej, Spółka dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Wzór rejestru naruszeń danych osobowych stanowi **Załącznik nr 9** do Polityki.

§ 11 Powierzenie przetwarzania

11.1. Spółka może powierzyć Przetwarzanie Danych osobowych Podmiotowi przetwarzającemu wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi w art. 28 ust. 3 RODO. Powierzenie Przetwarzania Danych osobowych, o którym mowa w zdaniu poprzedzającym nie może prowadzić do naruszenia tajemnicy doradcy podatkowego.

11.2. Spółka korzysta wyłącznie z usług takich Podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. W celu weryfikacji spełnienia obowiązku, o którym mowa w zdaniu poprzedzającym, Spółka przed powierzeniem przetwarzania potencjalnemu Podmiotowi przetwarzającemu w miarę możliwości uzyskuje informacje o zasadach ochrony Danych osobowych stosowanych przez potencjalny Podmiot przetwarzający, oraz o praktykach tego podmiotu dotyczących zabezpieczenia Danych osobowych.

§ 12 Przekazywanie danych do Państwa trzeciego

12.1. Spółka nie przekazuje Danych osobowych do państwa trzeciego położonego poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego, poza sytuacjami, w których następuje to na wniosek osoby, której Dane osobowe dotyczą.

12.2. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych, Spółka okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

§ 13 Postanowienia końcowe

13.1. Polityka wchodzi w życie z dniem ogłoszenia.

13.2. W sprawach nieuregulowanych w Polityce odpowiednie zastosowanie znajdują postanowienia RODO oraz powszechnie obowiązujące przepisy prawa polskiego i europejskiego.

13.3. Wszelkie zmiany lub uzupełnienia do Polityki wymagają dla swej skuteczności formy pisemnej pod rygorem nieważności. Zmiany lub uzupełnienia do Polityki wchodzą w życie nie wcześniej niż w terminie 7 dni od dnia ich ogłoszenia.

13.4. Do Polityki dołączono następujące Załączniki, stanowiące integralną część Polityki:

(i) Załącznik nr 1 – Lista podmiotów powiązanych ze Spółką kapitałowo lub osobowo

(ii) Załącznik nr 2 – Lista Zbiorów danych w Spółki;

(iii) Załącznik nr 3 – Wzór Upoważnienia do przetwarzania danych osobowych;

(iv) Załącznik nr 4 – Wzór Zobowiązania do zachowania poufności;

(v) Załącznik nr 5 – Polityka czystego biurka;

(vi) Załącznik nr 6 – Procedura otwierania i zamykania budynku oraz pomieszczeń

(vii) Załącznik nr 7 – Wzór rejestru czynności przetwarzania;

(viii) Załącznik nr 8 – Wzór zgłoszenia naruszenia ochrony danych osobowych;

(ix) Załącznik nr 9 – Wzór rejestru naruszeń danych osobowych;

Załącznik nr 1 - Lista podmiotów powiązanych kapitałowo lub osobowo ze Spółką

(i) **Centrum Finansowo-Księgowe EKKOM Sp. z o.o. Spółka Komandytowa**;
z siedzibą: ul. Krotoszyńska 55, 51-009 Wrocław
z miejscem prowadzenia działalności: ul. Robotnicza 68a, 53-608 Wrocław
KRS 0000555876

(ii) **Centrum Personalne EKKOM Sp. z o.o.**;
z siedzibą i miejscem prowadzenia działalności: ul. Robotnicza 68a, 53-608 Wrocław
KRS 0000615622

(iii) **Centrum Personalne EKKOM Sp. z o.o. Spółka Komandytowa;**
z siedzibą i miejscem prowadzenia działalności: ul. Robotnicza 68a, 53-608 Wrocław
KRS 0000713627

Załącznik nr 2 – Lista Zbiorów danych w Spółce

Uwzględniając definicję z art. 4 pkt 6 RODO, Spółka przetwarzana Dane osobowe zgrupowane w następujących Zbiorach danych:

(i) **Pracownicy Spółki** – obejmujący dane osobowe osób fizycznych zatrudnionych w Spółki na podstawie stosunku pracy (niezależnie od podstawy jego nawiązania), dane osobowe osób fizycznych współpracujących z Kancelarią na podstawie umowy cywilnoprawnej (umowy zlecenie, umowy o dzieło) oraz dane osobowe praktykantów i stażystów Spółki;

(ii) **Klienci** – obejmujący dane osobowe klientów Spółki będących osobami fizycznymi, w tym prowadzącymi jednoosobową działalność gospodarczą, jak również dane osobowe osób fizycznych będących przedstawicielami (reprezentantami) klientów Spółki (członkowie zarządów, prokurenci i pełnomocnicy osób prawnych; pracownicy klientów występujący w imieniu kontrahentów);

(iii) **Potencjalni Klienci –** obejmujący dane osobowe potencjalnych klientów Spółki będących osobami fizycznymi, w tym prowadzącymi jednoosobową działalność gospodarczą, jak również dane osobowe osób fizycznych będących przedstawicielami (reprezentantami) potencjalnych klientów Spółki (członkowie zarządów, prokurenci i pełnomocnicy osób prawnych; pracownicy klientów występujący w imieniu kontrahentów);

(iv) **Dostawcy** - obejmujący dane osobowe dostawców Spółki będących osobami fizycznymi prowadzącymi jednoosobową działalność gospodarczą, jak również dane osobowe osób fizycznych będących przedstawicielami (reprezentantami) dostawców Spółki (członkowie zarządów, prokurenci i pełnomocnicy osób prawnych; pracownicy dostawców występujący w imieniu kontrahentów);

(v) **Pracownicy klientów** – obejmujące dane osobowe pracowników oraz współpracowników Klientów obsługiwanych w zakresie kadrowo-płacowym przez Spółkę;

(vi) **Kontrahenci klientów –** obejmuje dane osobowe klientów i dostawców klientów obsługiwanych w zakresie księgowym przez Spółkę;

(vii) **Przedstawiciele organów** – obejmujący dane osobowe przedstawicieli organów administracji publicznej oraz sądów powszechnych, Sądu Najwyższego i sądów administracyjnych, występujących w imieniu takich organów lub sądów;

(viii) **Dane nieidentyfikowane** – Dane osobowe nieidentyfikowane przez Spółkę, takie jak dane osób monitorowanych przy wykorzystaniu monitoringu Spółki;

(ix) **Dane w aktach sprawy** – Dane osobowe osób fizycznych przetwarzane w związku z prowadzonymi przez Spółkę postępowaniami, kontrolami lub postępowaniami sądowymi (dane stron postępowania, dane pełnomocników stron, etc.).

Załącznik nr 3 – Wzór Upoważnienia do przetwarzania danych osobowych

[Miasto], dnia [Data]

Upoważnienie Pracownika
do przetwarzania danych osobowych

Działając w imieniu [Nazwa Spółki], na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1) (zwanego dalej RODO) – nadaję:

[Imię i nazwisko upoważnionego],

zatrudnionemu na stanowisku:

[Stanowisko]

upoważnienie do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych w zakresie [Opis zakresu dostępu do danych osobowych, np. bez ograniczeń, pogląd danych osobowych, wprowadzanie i opracowywanie danych, usuwanie danych].

Upoważnienie obejmuje przetwarzanie danych osobowych:

(i) przetwarzanych na nośnikach papierowych;
(ii) przetwarzanych w systemach informatycznych:
  (a) [•],
  (b) [•];
(iii) Dane osobowe objęte Zbiorami danych:
  (a) [•],
  (b) [•].

Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych w okresie zatrudnienia.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, Ustawy z dnia [Data Ustawy, po jej uchwaleniu] o ochronie danych osobowych, Kodeksu pracy, a także z Polityką ochrony danych osobowych Pracodawcy.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych u Pracodawcy.

Pracodawca _____

[Data i podpis]

Załącznik nr 4 – Wzór zobowiązania do zachowania poufności

[Miasto], dnia [Data]

Pracownik: [Dane pracownika]

Zobowiązanie do zachowania poufności

Oświadczam, że w związku z wykonywaniem obowiązków służbowych na rzecz [Nazwa Spółki] oraz udzielonym mi upoważnieniem do przetwarzania danych osobowych:

(i) zostałem/am poinformowany/a o zasadach przetwarzania i ochrony danych osobowych w [Nazwa Spółki], w tym o:
  (a) treści Polityki ochrony danych osobowych z dnia [Data Polityki],
  (b) procedurach oraz regulacjach dotyczących ochrony danych osobowych obowiązujących w Spółce, w tym:
    – Polityką czystego biurka z dnia [Data wprowadzenia],
    – Procedurą otwierania i zamykania budynku oraz pomieszczeń biurowych;
  (c) przepisach dotyczących ochrony tajemnicy zawodowej doradcy podatkowego,
  (d) zasadach ochrony danych osobowych wynikających z postanowień bezwzględnie obowiązującego prawa, w szczególności wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1);
(ii) treść informacji oraz regulacji, o których mowa w pkt (i) wyżej, oraz nałożonych na mnie na mocy Polityki obowiązków jest dla mnie jasna i zrozumiała.

W związku z powyższym zobowiązuje się do:

(i) niezwłocznego stosowania się do nałożonych na mnie obowiązków w zakresie ochrony danych osobowych;
(ii) zapewnienia ochrony, poufności oraz integralności danych osobowych przetwarzanych w zbiorach przez Spółkę, w szczególności do zapewnienia należytego bezpieczeństwa danych osobowych przed ich ujawnieniem lub udostępnieniem (nawet przypadkowym) osobom trzecim i osobom nieuprawnionym, jak również przed ich nieuprawnionym lub przypadkowym uszkodzeniem, utratą lub zmodyfikowaniem,
(iii) zachowania tajemnicy i poufności dotyczącej wszelkich informacji przetwarzanych w toku zatrudnienia w Spółce, w tym także po zaprzestaniu wykonywania prac;
(iv) zachowania w tajemnicy wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych w Spółce;

(v) niezwłocznego zgłaszania przełożonemu wszelkich naruszeń ochrony danych osobowych, jak również wszelkich zaobserwowanych prób lub faktów naruszenia zabezpieczeń pomieszczeń lub systemów informatycznych.

Pracownik _____

(data i podpis)

Załącznik nr 5 – Polityka czystego biurka

W Centrum Finansowo-Księgowym EKKOM Sp. z o.o. z dniem 25 maja 2018 r. wprowadza się Politykę Czystego Biurka. Polityka obejmuje wszystkich pracowników oraz współpracowników Spółki.

Nadzór nad wykonywaniem polityki powierza się Osobie wyznaczonej do tego celu przez Zarząd.

Polityka Czystego Biurka

1. Polityka reguluje wymagania oraz procedury ochrony danych poufnych, w tym danych osobowych przetwarzanych w Centrum Finansowo-Księgowym EKKOM Sp. z o.o. i spółkach powiązanych przez Pracowników w formie papierowej, w tym:
    a. dokumentów papierowych;
    b. korespondencji listownej;
    c. akt sprawy;
    d. dokumentów źródłowych przekazanych przez klientów Spółki;
    e. korespondencję urzędową.
2. Ilekroć w Polityce zostaną wykorzystane następujące definicje i zwroty, należy nadawać im następujące znaczenie:
    a. Polityka – oznacza niniejszą Politykę Czystego Biurka wraz ze wszystkimi ewentualnymi załącznikami;
    b. Pracownik – oznacza zarówno każdą osobę fizyczną zatrudnioną w Spółce, oraz w Spółkach powiązanych kapitałowo lub osobowo, na podstanie umowy o pracę, jak również współpracującą na podstawie umowy cywilnoprawnej (w tym w zakresie prowadzonej jednoosobowej działalności gospodarczej), studenta lub ucznia niebędących pracownikami Spółki w trakcie odbywania praktyk lub stażu zawodowego;
    c. Spółka – oznacza Centrum Finansowo-Księgowe EKKOM Sp. z o.o. i spółki powiązane.
3. Polityka obowiązuje wszystkich Pracowników Spółki, niezależnie od zajmowanego stanowiska i czasu zatrudnienia w Spółce.
4. Każdy Pracownik zobowiązany jest do ograniczenia dostępu osób postronnych do danych poufnych, w tym danych osobowych zawartych na nośnikach papierowych wykorzystywanych przez Pracownika przy wykonywaniu obowiązków służbowych.
5. W toku pracy każdy Pracownik zobowiązany jest do przechowywania na biurku lub przy stanowisku pracy tylko tych dokumentów, które są Pracownikowi niezbędne do wykonania bieżących zadań w danym momencie pracy. Jeżeli dane dokumenty nie będą już pracownikowi niezbędne do wykonania bieżących zadań, Pracownik zobowiązany jest do ich odłożenia. Postanowienia ust. 6 niżej stosuje się odpowiednio.

6. W przypadku opuszczenia przez pracownika – choćby chwilowo – biurka lub stanowiska pracy, Pracownik zobowiązany jest do odłożenia i schowania wszystkich wykorzystywanych dokumentów zawierających dane poufne lub dane osobowe do zamykanej szuflady lub szafy, celem uniemożliwienia dostępu do dokumentów osobom postronnym.
7. W przypadku zakończenia przez Pracownika pracy w danym dniu, Pracownik jest obowiązany przed opuszczeniem siedziby Spółki do wykonania obowiązku, o którym mowa w ust. 6 wyżej oraz do zabezpieczenia dokumentów przed dostępem jakichkolwiek osób postronnych. Po zakończonej pracy na biurku mogą znajdować się jedynie telefon stacjonarny i przybory biurowe.
8. Pracownik zobowiązany jest zapewnić, aby w toku pracy przy stanowisku pracy nie znajdowały się płyny lub inne substancje grożące zniszczeniem lub uszkodzeniem dokumentacji papierowej przy ich rozlaniu. Na tej samej podstawie Pracownik zobowiązany jest do powstrzymania się od spożywania posiłków przy biurku lub stanowisku pracy.
9. Niezależnie od postanowień ust. 4-8 wyżej, po zakończonej pracy Pracownik zobowiązany jest odłożyć laptop służbowy do zamykanej na klucz szafy, celem uniemożliwienia dostępu do danych zapisanych na komputerze służbowym osobom postronnym.
10. Jeżeli dany dokument nie będzie już wykorzystywany w Spółce, jak również w sytuacjach określonych w Polityce Ochrony Danych Osobowych z dnia 25 maja 2018 r., Pracownik zobowiązany jest do zapewnienia niezwłocznego zniszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, o ile Polityka Ochrony Danych Osobowych z dnia 25 maja 2018 r. nie przewiduje innego sposobu zadysponowania dokumentów lub nie nakazuje jego pozostawienia lub archiwizacji.

Załącznik nr 6 – Procedura otwierania i zamykania budynku oraz pomieszczeń biurowych

W Centrum Finansowo-Księgowym EKKOM Sp. z o.o. z dniem 25 maja 2018 r. wprowadza się procedurę otwierania i zamykania budynku oraz pomieszczeń biurowych położonych przy ul. Robotniczej 68a we Wrocławiu, zwaną dalej „Polityką kluczy".

Nadzór nad wykonywaniem polityki powierza się Osobie wyznaczonej do tego celu przez Zarząd.

Procedura otwierania i zamykania budynków oraz pomieszczeń biurowych

1) Procedura otwierania i przebywania w budynku

a) Miejscem prowadzenia działalności Centrum Finansowo-Księgowego EKKOM Sp. z o.o. jest lokal biurowy znajdujący się przy ul. Robotniczej 68a we Wrocławiu, zwany dalej: Lokalem.

b) Do otwierania oraz zamykania Lokalu uprawnione są osoby wskazane w Załącznik nr 1 do Procedury.

c) Po otwarciu Lokalu i wyłączeniu systemu alarmowego osoba uprawniona otwiera pomieszczenie, w którym znajduje się zamykana szuflada z kluczami do pozostałych pomieszczeń biurowych.

d) Z pomieszczenia tego pracownicy pobierają klucze do swojego pomieszczenia biurowego i kwitują ich odbiór w ewidencji kluczy.

e) W przypadku nieobecności osób posiadających klucze główne do budynku, Członek Zarządu może upoważnić innego pracownika do otwierania i zamykania lokalu oraz pomieszczeń biurowych.

f) W razie niemożności otwarcia lub zamknięcia budynku lub pomieszczeń biurowych, pracownik niezwłocznie zawiadamia o tym fakcie Członek Zarządu.

g) W pomieszczeniach biurowych, podczas godzin pracy, gdzie przebywa tylko jeden pracownik, jest on zobowiązany do każdorazowego zamknięcia pomieszczenia w przypadku jego opuszczenia, z wyłączeniem pomieszczeń, które łączą się z pomieszczeniami posiadającymi bezpośrednie wyjście na korytarz, pod warunkiem przebywania w pomieszczeniach innych pracowników.

h) Przebywanie pracowników w Lokalu po godzinach pracy powyżej 30 minut od zakończenia pracy jest niedozwolone, z zastrzeżeniem lit. i) oraz j) niżej.

i) Przebywanie pracowników w Lokalu po godzinach pracy lub dni wolne od pracy jest dopuszczalne wyłącznie za zgodą lub na podstawie pisemnego polecenia służbowego przełożonego, a w razie jego nieobecności osoby go zastępującej.

j) Od wymogów określonych w lit. h) wyżej zwolnieni są:

   i) Członkowie Zarządu,

   ii) kierownicy Zespołów,

   iii) inne osoby upoważnione pisemnie przez Członka Zarządu.

2) Procedura włączania i wyłączania systemów alarmowych.

a) Lokal podlega dozorowi i ochronie polegającej na całodobowym monitorowaniu systemu sygnalizacji alarmowo-włamaniowej oraz systemu sygnalizacji pożarowej przez firmę ochroniarską, na zasadach określonych w Umowach zawartych z tymi podmiotami.

b) Uprawnienia do włączenia i wyłączenia centralnego systemu alarmowego posiadają upoważnione osoby, wyszczególnione w Załącznik nr 1 do Procedury. Każda z tych osób posługuje się indywidualnym hasłem dostępu. System każdorazowo rejestruje datę, godzinę oraz osobę dokonującą czynności włączenia i wyłączenia alarmu.

c) Osoby posiadające hasła dostępu do systemu alarmowego zobowiązane są do zachowania szczególnej ostrożności w trakcie ich używania. Hasła dostępu stanowią tajemnicę służbową. Wykaz kodów alarmowych znajduje się w sejfie, w zamkniętej kopercie.

d) W przypadku wystąpienia alarmu w Lokalu firma ochroniarska powiadamia, według wskazanej kolejności, jedną z osób wyszczególnionych w Części 3 Załącznik nr 1 do Procedury. Do zadań tej osoby należy umożliwienie służbie patrolowej wejścia do budynku (poza godzinami urzędowania) i w zależności od sytuacji umożliwienie wejścia do pomieszczeń biurowych w celu weryfikacji i usunięcia przyczyn uruchomienia sygnalizacji alarmowej.

3) Procedura zamykania budynku i pomieszczeń.

a) Po zakończeniu pracy pracownicy mają obowiązek zamknąć pomieszczenia na klucz i odnotować ten fakt w Ewidencji pobierania i zdawania kluczy, której wzór Załącznik nr 2 do Procedury.

b) Osoba wymieniona w Załącznik nr 1 do Procedury ma obowiązek włączyć system alarmowy. Włączenie systemu alarmowego następuje po sprawdzeniu pomieszczeń biurowych, korytarzy oraz pomieszczeń sanitarnych znajdujących się w Lokalu i stwierdzeniu możliwości zamknięcia Lokalu.

c) Zamknięcie Lokalu następuje nie później niż o godzinie 16:30. W uzasadnionych przypadkach, za zgodą Członka Zarządu lub osoby go zastępującej godzina zamknięcia może ulec zmianie.

4) Procedura przechowywania i dysponowania kluczami.

a) W Centrum Finansowo-Księgowym EKKOM Sp. z o.o. prowadzona jest ewidencja pobierania i zdawania kluczy, wg wzoru stanowiącego Załącznik nr 2 do Procedury. Ewidencja przechowywana jest na recepcji.

b) Klucze do Lokalu i pomieszczeń biurowych przechowywane są na recepcji w zamykanej szufladzie, z wyłączeniem kluczy do archiwum.

c) Osoby dysponujące kluczami zobowiązane są do odpowiedniego zabezpieczenia kluczy przed ich zgubieniem i kradzieżą oraz ewidencji wejść do Lokalu.

d) W przypadku zagubienia, zaginięcia klucza lub stwierdzenia jego braku pracownik zgłasza ten fakt natychmiast Osobie nadzorującej i w razie konieczności wydania kluczy zapasowych składa w tej sprawie wniosek.

e) Wydawanie kluczy zapasowych pracownikowi może odbywać tylko w uzasadnionych sytuacjach za zgodą Członka Zarządu.

f) Klucze zapasowe do poszczególnych pomieszczeń biurowych przechowywane są w skrzynce metalowej znajdującej się w Sekretariacie. Klucz do skrzynki z kluczami zapasowymi posiadają osoby wymienione w Załącznik nr 1 do Procedury.

g) Zabrania się pracownikom samodzielnego dorabiania kluczy do Lokalu i pomieszczeń biurowych.

h) Zabrania się pozostawiania kluczy w zamkach od drzwi podczas obecności i nieobecności pracownika w pomieszczeniu biurowym.

i) Zabrania się udostępniania kluczy osobom nieupoważnionym.

5) Upoważnienia

a) Osoby wyszczególnione w Załącznik nr 1 Załącznik nr 1 - Wykaz osób uprawnionych;do Procedury otrzymują stosowne upoważnienia do posiadania kluczy. Wzór upoważnienia stanowi Załącznik nr 3 Załącznik nr 3 – Wzór upoważnienia do posiadania kluczydo Procedury.

b) Upoważnienia wpina się do segregatora upoważnień, który znajduje się w gabinecie Zarządu.

6) **Postanowienia końcowe**

a) Do Procedury dołączono następujące Załączniki:

i) Załącznik nr 1 - Wykaz osób uprawnionych;

ii) Załącznik nr 2 – Ewidencja pobierania i zdawania kluczy do pomieszczeń biurowych;

iii) Załącznik nr 3 – Wzór upoważnienia do posiadania kluczy

Załącznik nr 1

do Procedury otwierania i zamykania budynku oraz pomieszczeń biurowych

Wykaz osób uprawnionych

Część 1 Wykaz osób stale uprawnionych do otwierania i zamykania Lokalu

*Następujące osoby posiadają **stały dostęp** do Lokalu (dysponują indywidualnym kodem dostępu oraz kompletem kluczy, w tym do skrzynek z kluczami):*

(i) [•];

(ii) [•];

(iii) [•].

Część 2 Wykaz osób stale uprawnionych do otwierania i zamykania Lokalu

*Następujące osoby posiadają **czasowy dostęp** do Lokalu (dysponują indywidualnym kodem dostępu oraz kompletem kluczy, w tym do skrzynek z kluczami):*

(i) [•];

(ii) [•];

(iii) [•].

Część 3 Osoby zawiadamiane w przypadku alarmu

W przypadku aktywowania alarmu w Lokalu, firma ochroniarska zawiadamia następujące osoby:

(i) [•];

(ii) [•];

(iii) [•].

Załącznik nr 2
do Procedury otwierania i zamykania budynku oraz pomieszczeń biurowych

Ewidencja pobierania i zdawania kluczy w Lokalu

Nr Klucza	***Godzina pobrania klucza***	***Czytelny podpis osoby pobierającej klucz***	***Godzina zdania klucza***	***Czytelny podpis osoby przyjmującej klucz***	***Uwagi***

Załącznik nr 3
do Procedury otwierania i zamykania budynku oraz pomieszczeń biurowych

[Miasto], dnia [Data]

Upoważnienie do posiadania kluczy

Działając w imieniu [Nazwa Spółki] niniejszym upoważniam Pracownika [Imię i nazwisko Pracownika] do stałego/czasowego posiadania kompletu kluczy głównych do Lokalu w ilości [•] sztuk, jak również do dysponowania kodem alarmowym niezbędnym do uzbrojenia oraz rozbrojenia alarmu zainstalowanego w Lokalu.

Odbiór i zwrot kluczy kwitowany jest w Ewidencji pobierania i zdawania kluczy w Lokalu.

Pracownik zobowiązany jest do odpowiedniego zabezpieczenia kluczy przed zgubieniem i kradzieżą.

_____
[Data i podpis Właściciela/Członka Zarządu]

Niniejszym potwierdzam zapoznanie się z treścią upoważnienia oraz zobowiązania, jak również otrzymanie kluczy w ilości [•] sztuk, w tym:

(i) do drzwi głównych – [•]sztuk,
(ii) do skrzynki systemu alarmowego – [•] sztuk,
(iii) po pomieszczeń biurowych – [•] sztuk,
(iv) [•]

_____
[Data i podpis Pracownika]

Załącznik nr 7 – Wzór Rejestru Czynności Przetwarzania

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
LP.	**Nazwa czynności przetwarzania**	**Jednostka organizacyjna (departament, dział itp.)**	**Cel przetwarzania**	**Kategorie osób**	**Kategorie danych**	**Podstawa prawna**	**Źródło danych**	**Przepływ danych**	**Planowany termin usunięcia kategorii danych** *(jeżeli jest to możliwe)*	**Nazwa współadministratora i dane kontaktowe** *(jeśli dotyczy)*	**Nazwa podmiotu przetwarzającego i dane kontakowe** *(jeśli dotyczy)*	**Kategorie odbiorców** *(innych niż podmiot przetwarzający)*	**Nazwa systemu lub oprogramowania**	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1** ***(jeżeli jest to możliwe)***	**DPIA (jeśli tak, lokalizacja raportu)**	Transfer do kraju trzeciego lub org. międzynarodowej	
																Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	**Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń**
			Art.. 30 ust. 1 pkt b	**Art.. 30 ust. 1 pkt c**	**Art.. 30 ust. 1 pkt c**				**Art.. 30 ust. 1 pkt f**	**Art.. 30 ust. 1 pkt a**	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt d**		**Art.. 30 ust. 1 pkt g**		**Art. 30 ust. 1 pkt e**	**Art. 30 ust. 1 pkt e**
1.																	
2.																	
3.																	
4.																	
5.																	
6.																	
7.																	

Załącznik nr 8 - Wzór zgłoszenia naruszenia ochrony danych osobowych

[Miejscowość], dnia [Data]

[Nazwa Spółki]
[Adres Spółki]
[Adres Spółki]

Prezes Urzędu Ochrony Danych Osobowych
[Adres organu]
[Adres organu]

Zgłoszenie naruszenia ochrony danych osobowych

Działając w imieniu Spółki [Nazwa Spółki] z siedzibą w [Siedziba], w oparciu o przyznane mi uprawnienia oraz na podstawie art. 33 ust. 1 i 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1), niniejszym zgłaszam następujące naruszenie ochrony danych osobowych:

Administrator Danych Osobowych oraz dane kontaktowe naruszenia:	
Data zaistnienia naruszenia:	
Kategorie i przybliżoną liczbę osób, których dane dotyczą:	
Kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie:	
Opisywać możliwe konsekwencje naruszenia ochrony danych osobowych:	
Opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych	

_____

[Podpis osoby upoważnionej]

Załącznik nr 9 – Wzór rejestru naruszeń ochrony danych osobowych

Lp.	Opis naruszenia	Data zajścia naruszenia	Kategoria i ilość osób, których dotyczy naruszenie	Zakres danych i/lub kategorie danych, których dotyczy naruszenie	Okoliczności naruszenia - opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia	Opis skutków/konsekwencji naruszenia	Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowane środki zastosowane w celu zminimalizowania jego negatywnych skutków	Rezultat działań naprawczych