Polityka Ochrony Danych Osobowych
z dnia 25.05.2018 r.

Faber Spółką z ograniczoną odpowiedzialnością, wpisana do rejestru przedsiębiorców KRS 0000144853, prowadzonego przez Sąd Rejonowy dla Krakowa – Śródmieścia w Krakowie, Wydział XI Gospodarczy, z kapitałem zakładowym w wysokości 50 000,00 PLN, (opłaconym w całości) i zarządem w składzie: Monika Kuśmider, Piotr Koźmiński, Paweł K. Koźmiński – prezes, **prowadzącą Kancelarię Rachunkową** z siedzibą w Krakowie, ul. Mysłakowskiego 9; NIP 6761027406; Regon 350892160 (zwana dalej Kancelarią), 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), (zwanego dalej: RODO) mając również na uwadze prawodawstwo krajowe, celem zapewnienia, że Dane Osobowe (zwane dalej DO) w Kancelarii Rachunkowej (zwana dalej Kancelarią) są przetwarzane i zabezpieczone zgodnie z postanowieniami prawa, oraz zgodnie z przyjętą i obowiązującą w Kancelarii normą ISO 9001:2008 poprzez wdrożenia odpowiednich środków technicznych i organizacyjnych zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń; a Kancelaria zapewnia, że domyślnie przetwarzane były wyłącznie te DO, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

I. Postanowienia wstępne:

1. Polityka określa zasady przetwarzania oraz zabezpieczania DO w Kancelarii, celem zapewnienia zbieżności Przetwarzania z wymaganiami RODO oraz przepisami bezwzględnie obowiązującego prawa polskiego w zakresie przetwarzania DO.
   Polityka ta wraz z Systemem Zarządzania Jakością ISO 9001:2008 (zwanym dalej SZJ) stanowi zbiór oraz podstawę wdrożonych w Kancelarii wymogów, procedur oraz zasad ochrony DO. Polityka zawiera:
   1. zawiera opis zasad ochrony DO obowiązujący w Kancelarii;
   2. zbiór procedur, instrukcji i regulacji szczegółowych dotyczących przetwarzania DO w Kancelarii, dotyczących poszczególnych obszarów z zakresu ochrony DO; stanowiących załączniki do Polityki.
   3. Polityka obowiązuje wszystkich pracowników oraz współpracowników Kancelarii. Za przestrzeganie i utrzymanie postanowień Polityki odpowiedzialni są:
      1. Zarząd i Prokurenci Kancelarii;
      2. Inspektor DO powołany przez Kancelarię (zwanym dalej IDO)
      3. Pełnomocnik ds. SZJ Kancelarii;
      4. Pracownicy.
      5. Stażyści i praktykanci.
      6. Personel pomocniczy i kooperanci (w tym personel IT).
   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 Kancelaria zapewnia:
      1. Wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania DO z wymogami prawa oraz niezbędne zabezpieczenie przetwarzanych DO.
      2. Stałe monitorowanie zgodności przetwarzania DO z wymogami prawa oraz poddawanie środków, o których mowa w ust. 1 powyżej okresowym przeglądom oraz uaktualnianiu;
      3. Kontrolę i nadzór nad przetwarzaniem DO.
      4. Nadzór nad przestrzeganiem postanowień polityki zapewnia Zarząd Kancelarii wraz z IDO.
         Nadzór, o którym mowa w zdaniu poprzedzającym zmierza w szczególności, ale nie wyłącznie do zapewnienia, że czynności związane z przetwarzaniem DO w Kancelarii są zgodne z wymogami prawa, postanowieniami Polityki oraz SZJ.
      5. Kancelaria zapewnia zgodność postępowania kontrahentów Kancelarii, w tym w szczególności Podmiotów Przetwarzających z postanowieniami Polityki w odpowiednim zakresie we wszystkich sytuacjach, w których dochodzi do przekazania tym podmiotom DO do przetwarzania, w tym przechowywania.
      6. Polityka jest przechowywana i udostępniana w wersji papierowej oraz elektronicznej w siedzibie Kancelarii.
         1. Politykę udostępnia się:
            1. Obligatoryjnie wszystkim osobom upoważnionym do przetwarzania DO w Kancelarii, celem zapewnienia osobom upoważnionym należytej wiedzy oraz informacji na temat zasad i wymogów dotyczących przetwarzania DO w Kancelarii.
            2. Klientom Kancelarii.
            3. Stałym współpracownikom Kancelarii, w tym personelowi IT.
            4. Osobom zainteresowanym, w szczególności osobom fizycznym, których dane dotyczą – na ich wniosek.

II. Słownik pojęć:

1. Ilekroć w niniejszej Polityce zostaną wykorzystane poniższe definicje lub zwroty, należy nadawać im następujące znaczenie:
    1. Polityka – oznacza niniejszą Politykę wraz ze wszystkimi ewentualnymi Załącznikami;
    2. Dane Osobowe (DO) – 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;
    3. Dane wrażliwe – oznaczają DO, o których mowa w art. 9 RODO.
    4. RODO – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem DO 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);
    5. Osoba upoważniona – oznacza osobę upoważnioną przez Kancelarię do przetwarzania DO w danym zakresie;
    6. Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na DO lub zestawach DO 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;
    7. Zbiór danych – oznacza każdy uporządkowany zestaw DO, dostępny według określonych kryteriów;
    8. Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza DO w imieniu i na rzecz Kancelarii.
    9. Rejestr - oznacza Rejestr Czynności Przetwarzania DO Kancelarii.
    10. Uwierzytelnienie – oznacza działanie, którego celem jest weryfikacja deklarowanej tożsamości Użytkownika;
    11. Kancelaria – oznacza właściciela niniejszej Polityki wymienionego w preambule.
    12. Klient - osoba lub podmiot, która jest związany umową o świadczenie usług z Kancelarią,
    13. Pracownicy – oznaczają zarówno osoby zatrudnione w Kancelarii na podstawie stosunku pracy, jak również osoby fizyczne współpracujące z Kancelarią na podstawie Umowy cywilnoprawnej;
    14. System – oznacza System ochrony DO w Kancelarii, o którym mowa w niniejszej Polityce;
    15. Umowa Główna – umowa pomiędzy Klientami a Kancelarią dotycząca świadczenia usług z zakresu rachunkowości oraz kadrowo-płacowych.
    16. SWI – System Wymiany Informacji – pomiędzy Klientami a Kancelarią – pomiędzy Klientami a Kancelarią zgodnie z załącznikiem nr 1 stanowiącym Regulamin korzystania z SWI do Umowy Głównej.
    17. ISO – System Zarządzania Jakością ISO 9001:2018 uzyskany i potwierdzony Certyfikatem nr 9190 FBR1 IT 52859.

III Dane Osobowe:

1. Kancelaria przetwarza DO dostarczone przez Klienta, oraz własne, gromadzone w zbiorach danych. Zbiory danych przetwarzane w Kancelarii to:
    1. **Pracownicy Kancelarii** – obejmujący dane osobowe osób fizycznych zatrudnionych w Kancelarii na podstawie stosunku pracy (niezależnie od podstawy jego nawiązania), DO osób fizycznych współpracujących z Kancelarią na podstawie umowy cywilnoprawnej (umowy zlecenie, umowy o dzieło) oraz DO praktykantów i stażystów Kancelarii;
    2. **Klienci** – obejmujący DO klientów Kancelarii będących osobami fizycznymi, w tym prowadzącymi jednoosobową działalność gospodarczą, jak również DO osób fizycznych będących przedstawicielami (reprezentantami) klientów Kancelarii (członkowie zarządów, prokurenci i pełnomocnicy osób prawnych; pracownicy Klientów występujący w imieniu Klientów);
    3. **Dostawcy** - obejmujący DO dostawców Kancelarii będących osobami fizycznymi prowadzącymi jednoosobową działalność gospodarczą, jak również DO osób fizycznych będących przedstawicielami (reprezentantami) dostawców Kancelarii (członkowie zarządów, prokurenci i pełnomocnicy osób prawnych; pracownicy dostawców występujący w imieniu kontrahentów);
    4. **Pracownicy Klientów** – obejmujące dane osobowe pracowników oraz współpracowników Klientów obsługiwanych w zakresie kadrowo-płacowym przez Kancelarię;
    5. **Przedstawiciele organów** – obejmujący dane osobowe przedstawicieli organów administracji publicznej oraz sądów powszechnych, Sądu Najwyższego i sądów administracyjnych, występujących w imieniu takich organów lub sądów;
    6. **Dane nieidentyfikowane** – Dane osobowe nieidentyfikowane przez Kancelarię, takie jak dane osób monitorowanych przy wykorzystaniu monitoringu Kancelarii;
    7. **Dane w aktach sprawy** – DO osób fizycznych przetwarzane w związku z prowadzonymi przez Kancelarię postępowaniami, kontrolami lub postępowaniami sądowymi (dane stron postępowania, dane pełnomocników stron, etc.).
2. Uaktualnienie lub poszerzenie listy Zbiorów danych następuje po uprzednim przeprowadzeniu analizy skutków oraz ryzyk przetwarzania DO dla praw i wolności osób fizycznych objętych zbiorem.
3. Kancelaria nie podejmuje czynności Przetwarzania, które mogłyby wiązać się z istotnym ryzykiem naruszenia praw i wolności osób, których DO dotyczą. W przypadku planowania podjęcia czynności, o których mowa w zdaniu poprzedzającym Kancelaria obligatoryjnie przeprowadza uprzednią ocenę skutków przetwarzania, o których mowa w art. 35 RODO.

4. DO domyślnie Przetwarzane są na obszarze obejmującym pomieszczenia biurowe Kancelarii zlokalizowane w siedzibie Kancelarii zamieszczone w preambule. Dodatkowy obszar, w którym przetwarzane są DO, stanowią inne nośniki danych znajdujące się poza obszarem wskazanym w zdaniu poprzedzającym, jako kopie bezpieczeństwa.

IV. Podstawy ochrony DO w Kancelarii:

1. Kancelaria zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.
2. Osoby upoważnione oraz wszystkie inne osoby, którym udostępnia się DO Przetwarzane w Kancelarii zobowiązane są do Przetwarzania DO zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych wewnętrznych aktów prawnych Kancelarii lub procedur wewnętrznych związanych z Przetwarzaniem DO.
3. Przy zatrudnianiu Pracowników oraz w toku zatrudnienia Kancelaria zapewnia, że:
    1. Pracownicy przez przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad Przetwarzania i ochrony DO w Kancelarii;
    2. Każdy z Pracowników zostaje upoważniony na piśmie do Przetwarzania DO w niezbędnym zakresie, zgodnie z wzorem stanowiącym Załączniki nr 1 do Polityki;
    3. Każdy z pracowników zostaje zobowiązany do zachowania poufności i integralności DO, zgodnie z wzorem stanowiącym Załącznik nr 2 do Polityki, przy czym Pracownicy zobowiązani są w szczególności, ale nie wyłącznie do:
        1. Ścisłego przestrzegania zakresu upoważnienia;
        2. Przestrzegania wymogów prawa oraz postanowień Polityki w zakresie przetwarzania;
        3. Zachowania w tajemnicy DO;
        4. Zachowania w tajemnicy sposób zachowania poufności i integralności DO;
        5. Niezwłocznego zgłaszania Kancelarii wszelkich incydentów związanych z naruszeniem bezpieczeństwa DO.
        6. Kancelaria zapewnia, aby DO Przetwarzane w Kancelarii były:
            1. Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
            2. Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
            3. Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
            4. Prawidłowe i w razie potrzeby uaktualniane; Kancelaria podejmie bezzwłocznie wszelkie rozsądne działania, aby DO, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");
            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;
            6. Przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo DO, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.
    4. Przy zapewnieniu Przetwarzania DO zgodnie z zasadami wskazanymi w ustępie 1 powyżej Kancelaria opiera Przetwarzanie na następujących podstawach:
        1. Legalność – Kancelaria dba o ochronę prywatności i przetwarza DO zgodnie z wymogami prawa i przepisów wewnętrznych;
        2. Bezpieczeństwo − Kancelaria zapewnia odpowiedni poziom bezpieczeństwa DO podejmując stale działania w tym zakresie;
        3. Prawa Jednostki − Kancelaria umożliwia osobom, których DO są przetwarza, wykonywanie swoich praw i prawa te realizuje;
        4. Rozliczalność – Kancelaria zapewnia udokumentowanie sposobu spełniania obowiązków w zakresie ochrony DO.
        5. Kancelaria nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej.

V. System ochrony DO:

1. Kancelaria zapewnia zgodność Przetwarzania DO 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:
    1. Ograniczenie dostępu do pomieszczeń roboczych Kancelarii, poprzez karty magnetyczne lub kody PIN, w których przetwarzane są DO, jedynie do Osób upoważnionych oraz zapewnienie, że inne osoby mogą przebywać w pomieszczeniach wyłącznie w towarzystwie Osoby upoważnionej;
    2. Zamykanie pomieszczeń Kancelarii na czas nieobecności Pracowników, w sposób uniemożliwiający dostęp do nich osobom trzecim;
    3. Zapewnienie zabezpieczenia pomieszczeń Kancelarii przed czynnikami losowymi, takimi jak pożar lub powódź;
    4. Wykorzystywanie zamykanych szafek, szuflad lub innych środków technicznych uniemożliwiających osobom niepowołanym dostęp do przechowywanych w nich DO;

5. Wdrożenie Polityki czystego biurka, która stanowi Załącznik nr 3 do Polityki;
6. Wykorzystywanie wdrożonej Procedury otwierania i zamykania budynków oraz pomieszczeń biurowych, która stanowi Załącznik nr 5 do Polityki;
7. Zapewnienie skutecznego usuwania lub niszczenia dokumentów zawierających DO, w sposób uniemożliwiający ich późniejsze odtworzenie;
8. Zapewnienie bezpieczeństwa sprzętowego i informatycznego, obejmującego:
    1. Ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz.
    2. Zapewnienie aktualności stosowanego oprogramowania.
    3. Zabezpieczenie sprzętu komputerowego wykorzystywanego w Kancelarii przed złośliwym oprogramowaniem.
    4. Zapewnienie stałego i częstotliwego sporządzania kopii zapasowych danych przechowywanych na serwerze Kancelarii,
    5. Ograniczenie dostępu do systemu informatycznego poprzez stosowanie reguł Uwierzytelniania zgodnych z pilotką haseł.
    6. Przeprowadzanie analizy ryzyka dla czynności przetwarzania danych lub ich kategorii.
    7. Realizację standardów weryfikacji i doboru Podmiotów przetwarzających, jak również warunków powierzenia Przetwarzania danych na rzecz poszczególnych Podmiotów przetwarzających;
    8. Monitorowanie zmian w zakresie procesów Przetwarzania DO w Kancelarii oraz na bieżąco zarządza zmianami mającymi wpływ na ochronę DO w Kancelarii.

VI. Rejestr:

1. Rejestr obejmuje kategorie czynności przetwarzania DO w Kancelarii. Za pośrednictwem Rejestru Kancelaria dokumentuje czynności przetwarzania DO oraz inwentaryzuje i monitoruje sposób, w jaki wykorzystuje DO. Rejestr stanowi Załącznik nr 5 do Polityki.
2. Za pośrednictwem Rejestru, w szczególności poprzez wskazanie w Rejestrze ogólnych środków ochrony DO objętych wyodrębnioną czynnością przetwarzania, Kancelaria dąży również do wykazania zgodności Przetwarzania DO z wymogami prawa.
3. W Rejestrze, odrębnie dla każdej zidentyfikowanej kategorii czynności przetwarzania DO, odnotowuje się co najmniej:
    1. Nazwę czynności;
    2. Cel przetwarzania;
    3. Opis kategorii osób, których DO przetwarzane są w ramach danej czynności;
    4. Opis kategorii DO przetwarzanych w ramach danej czynności;
    5. Podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Kancelarii, jeśli podstawą przetwarzania jest uzasadniony interes;
    6. Opis kategorii odbiorców danych, w tym Podmiotów przetwarzających,
    7. Informację o ewentualnym przekazaniu DO poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;
    8. Ogólny opis technicznych i organizacyjnych środków ochrony DO, znajdujących zastosowanie do danej czynności.
4. W przypadku uaktualnienia lub poszerzenia kategorii czynności przetwarzania DO, Kancelaria dokonuje niezwłocznego uaktualnienia Rejestru celem zapewnienia zgodności Rejestru ze stanem faktycznym oraz zakresem operacji przetwarzania DO w Kancelarii.
5. Postanowienia ustępu 3 powyżej nie wyłączają możliwości ujęcia w Rejestrze w miarę potrzeby informacji dodatkowych, zwiększających szczegółowość lub czytelność Rejestru lub ułatwiających zarządzanie zgodnością ochrony DO z wymogami prawa, oraz realizację zasady rozliczalności.
6. Kancelaria 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 Kancelarię, uzasadniony cel Kancelarii.
7. Przepisy niniejszego rozdziału zaczną obowiązywać w sytuacji w której u któregokolwiek z Klientów nastąpi przekroczenie progu powodującego obowiązek prowadzenia rejestru. Do tego momentu stosowanie rozdziału VI. Zostaje zawieszone.

VII. Realizacja obowiązków wobec osób, których DO dotyczą:

1. Kancelaria wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (system SWI, email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności, takich jak zgłoszenie sprzeciwu lub ograniczenie przetwarzania.
2. Kancelaria dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których DO przetwarza.
3. Kancelaria publikuje w systemie SWI Kancelarii oraz pozostawia do wglądu w siedzibie Kancelarii:
    1. Politykę;
    2. Informację o prawach osób, których dane dotyczą;
    3. Informację o zakresie przetwarzanych DO w poszczególnych celach;
    a na ogólnodostępnej stronie:
    4. Metodach kontaktu z Kancelarią w zakresie DO;

4. W celu realizacji praw osoby, której DO dotyczą Kancelaria zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Kancelarię, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.
5. Kancelaria dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób, informując osobę, której dane dotyczą:
    1. O przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
    2. O przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
    3. O planowanej zmianie celu przetwarzania danych.
    4. Przed uchyleniem ograniczenia przetwarzania.
    5. O sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
    6. O prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
6. Kancelaria bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony DO, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
7. Niezależnie od postanowień ustępu 5 powyżej, Kancelaria informuje o przetwarzaniu danych niezidentyfikowanych poprzez publicznie dostępne tabliczki o monitoringu audio-wizualnym.
8. Na żądanie osoby dotyczące dostępu do jej danych, Kancelaria 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.
9. Dostęp do danych może być zrealizowany przez wydanie kopii danych, za sporządzenie kopii Kancelaria może pobrać opłatę zgodną z cennikiem usług publikowanym na stronie Kancelarii.
10. Kancelaria wydaje osobie, której DO dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.
11. Kancelaria dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której DO dotyczą. Kancelaria ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Kancelaria informuje osobę o odbiorcach danych, na żądanie tej osoby.
12. Kancelaria uzupełnia i aktualizuje dane na żądanie osoby, której DO dotyczą. Kancelaria ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Kancelaria może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Kancelarię procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
13. Z uwzględnieniem ustępu 14 poniżej na żądanie osoby, Kancelaria usuwa dane, gdy:
    1. Dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach.
    2. Zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania.
    3. Osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych.
    4. Dane były przetwarzane niezgodnie z prawem.
    5. Konieczność usunięcia wynika z obowiązku prawnego.
    6. Żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
14. Kancelaria przy usuwaniu DO 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.
15. Jeżeli dane podlegające usunięciu zostały upublicznione przez Kancelarię, Kancelaria podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te DO, o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Kancelaria informuje osobę o odbiorcach danych, na żądanie tej osoby.
16. Kancelaria dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
    1. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość.
    2. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu DO, żądając w zamian ograniczenia ich wykorzystywania.
    3. Kancelaria nie potrzebuje już DO, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń.
    4. 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.
17. W trakcie ograniczenia przetwarzania Kancelaria 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.
18. Na żądanie osoby Kancelaria 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 Kancelarii, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Kancelarii.
19. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, o którym mowa w art. 21 RODO, a dane przetwarzane są przez Kancelarię w oparciu o uzasadniony interes Kancelarii lub o powierzone Kancelarii zadanie w interesie publicznym, Kancelaria zobowiązuje się uwzględnić sprzeciw, o ile nie zachodzą po stronie Kancelarii ważne prawnie

uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

VIII. Minimalizacja danych:

1. Kancelaria wdraża procedury służące realizacji zasady minimalizacji przetwarzanych DO pod względem:
    1. Adekwatności DO do celów Przetwarzania, obejmujących ograniczenie ilości przetwarzanych DO oraz zakresu przetwarzania do celu Przetwarzania.
    2. Ograniczenia dostępu do DO wyłącznie do Osób upoważnionych, dla których wykorzystanie DO w określonym zakresie jest niezbędne dla prawidłowej realizacji obowiązków.
    3. Ograniczenia czasu przechowywania DO do okresu, dla którego przechowywanie DO jest niezbędne ze względu na realizację celu Przetwarzania lub obowiązków nałożonych na Kancelarię.
2. Kancelaria dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
3. Kancelaria stosuje ograniczenia dostępu do DO poprzez wdrożenie:
    1. Zobowiązanie Pracowników do zachowania poufności, a szczególnie w zakresie DO.
    2. Weryfikację kręgu wewnętrznych odbiorców DO poprzez nadawanie poszczególnym Pracownikom szczegółowych upoważnień co do Przetwarzania DO.
    3. Wdrożenie logicznych środków technicznych ochrony DO poprzez ograniczenie dostępu do systemów, oprogramowania oraz zasobów sieciowych wykorzystywanych w procesie Przetwarzania DO.
    4. Wdrożenie fizycznych środków technicznych ochrony DO, wskazanych w Polityce.
4. Kancelaria dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających. Kancelaria dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
5. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Kancelarii.
6. Kancelaria przetwarza DO z uwzględnieniem kryteriów wskazanych w Rejestrze. Kancelaria wdraża mechanizmy kontroli cyklu życia DO w Kancelaria, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.
7. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów Kancelarii, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Kancelarię. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

IX. Bezpieczeństwo DO:

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 Kancelaria wdraża środki techniczne i organizacyjne zapewniające należyty stopień ochrony DO, odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania DO przez Kancelarię.
2. Kancelaria przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa DO. W tym celu:
    1. Kancelaria kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
    2. Kancelaria przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Spółka analizuje możliwe sytuacje i scenariusze naruszenia ochrony DO uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
    3. Kancelaria wdraża środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności DO i dostępu do nich w razie incydentu fizycznego lub technicznego.

X. Naruszenie ochrony DO:

1. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony DO uważa się w szczególności, ale nie wyłącznie:
    1. Naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są DO.
    2. Przypadkowe udostępnienie DO osobom nieupoważnionym.
    3. Przetwarzanie DO niezgodnie z założonym zakresem i celem ich Przetwarzania.
    4. Nieuprawnione lub przypadkowe uszkodzenie, utratę, zniszczenie lub zmianę DO.
2. W przypadku stwierdzenia naruszenia ochrony DO Kancelaria dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych oraz szacuje skalę ryzyka.
3. W przypadku naruszenia ochrony DO, Kancelaria 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 6 do Polityki.
4. Jeżeli ryzyko naruszenia praw i wolności osoby, której DO dotyczą jest wysokie, Kancelaria zawiadamia o incydencie także osobę, której danej dotyczą, chyba że:

1. Kancelaria posiada wdrożone odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do DO, których dotyczy naruszenie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych DO.
2. Kancelaria zastosuje następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; lub
3. 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.

5. Niezależnie od obowiązków wskazanych powyżej, Kancelaria dokumentuje wszelkie naruszenia ochrony DO, w tym okoliczności naruszenia ochrony DO, jego skutki oraz podjęte działania naprawcze. Wzór rejestru naruszeń DO stanowi Załącznik nr 7 do Polityki.

XI. Powierzenie przetwarzania:

1. Kancelaria może powierzyć Przetwarzanie DO Podmiotowi przetwarzającemu wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi w art. 28 ust. 3 RODO. Powierzenie Przetwarzania DO, o którym mowa w zdaniu poprzedzającym nie może prowadzić do naruszenia tajemnicy doradcy podatkowego.
2. Kancelaria 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, Kancelaria przed powierzeniem przetwarzania potencjalnemu Podmiotowi przetwarzającemu w miarę możliwości uzyskuje informacje o zasadach ochrony DO stosowanych przez potencjalny Podmiot przetwarzający, oraz o praktykach tego podmiotu dotyczących zabezpieczenia DO.

XII. Przekazywanie danych do Państwa trzeciego:

1. Kancelaria nie przekazuje DO do państwa trzeciego położonego poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego, poza sytuacjami, w których następuje to na wniosek osoby, której DO dotyczą.
2. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych, Kancelaria okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

XIII. Postanowienia końcowe:

1. Polityka wchodzi w życie z dniem ogłoszenia.
2. W sprawach nieuregulowanych w Polityce odpowiednie zastosowanie znajdują postanowienia RODO oraz powszechnie obowiązujące przepisy prawa polskiego i europejskiego.
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.
4. Do Polityki dołączono następujące Załączniki, stanowiące integralną część Polityki:
    1. Załącznik nr 1 – Wzór Upoważnienia do przetwarzania DO.
    2. Załącznik nr 2 – Wzór Zobowiązania do zachowania poufności.
    3. Załącznik nr 3 – Polityka czystego biurka.
    4. Załącznik nr 4 – Procedura otwierania i zamykania budynku oraz pomieszczeń.
    5. Załącznik nr 5 – Rejestr Czynności Przetwarzania.
    6. Załącznik nr 6 – Wzór zgłoszenia naruszenia ochrony DO.
    7. Załącznik nr 7 – Rejestr naruszeń DO.

Kraków, dnia …..... r.

Załącznik nr 1
Wzór Upoważnienia do przetwarzania DO

Pracownik:

Upoważnienie Pracownika do przetwarzania DO

Działając w imieniu i na rzecz Kancelarii Rachunkowej 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 DO 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:

ww. pracownikowi zatrudnionemu na stanowisku księgowego, upoważnienie do przetwarzania DO w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania DO w zakresie niezbędnym do obsługi Klienta, z wyłączeniem usuwania danych.

Upoważnienie obejmuje przetwarzanie DO:

1. przetwarzanych na nośnikach papierowych;
2. przetwarzanych w systemach teleinformatycznych Kancelarii:
3. DO o objęte Zbiorami danych:
    1. Klienci – w zakresie powierzonych do przetwarzania.
    2. Pracownicy Klientów – w zakresie powierzonych do przetwarzania.
    3. Przedstawiciele organów – w zakresie kontaktów bezpośrednich w sprawach Klientów wymienionych pkt. 1.

Upoważnienie obejmuje uprawnienie do przetwarzania DO w okresie zatrudnienia.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania DO, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO zgodnie z rozporządzeniem i przepisami krajowymi, Kodeksu pracy, a także z Polityką ochrony DO 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.

….....
za Pracodawcę

Kraków, dnia …..... r.

Załącznik nr 2
Wzór zobowiązania do zachowania poufności

Pracownik:

Zobowiązanie do zachowania poufności

Oświadczam, że w związku z wykonywaniem obowiązków służbowych na rzecz Kancelarii Rachunkowej oraz udzielonym mi upoważnieniem do przetwarzania DO:

1. zostałem/am poinformowany/a o zasadach przetwarzania i ochrony DO w tym o:
    1. Treści Polityki ochrony DO.
    2. Procedurach oraz regulacjach dotyczących ochrony DO obowiązujących w Kancelarii,
    3. Przepisach dotyczących ochrony tajemnicy zawodowej.
    4. Zasadach ochrony DO 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 DO 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);
2. Treść informacji oraz regulacji, o których mowa powyżej, oraz nałożonych na mnie na mocy Polityki obowiązków jest dla mnie jasna i zrozumiała.

W związku z powyższym zobowiązuje się do:

1. Niezwłocznego stosowania się do nałożonych na mnie obowiązków w zakresie ochrony DO.
2. Zapewnienia ochrony, poufności oraz integralności DO przetwarzanych w zbiorach przez Kancelarię, w szczególności do zapewnienia należytego bezpieczeństwa DO przed ich ujawnieniem lub udostępnieniem (nawet przypadkowym) osobom trzecim i osobom nieuprawnionym, jak również przed ich nieuprawnionym lub przypadkowym uszkodzeniem, utratą lub zmodyfikowaniem.
3. Zachowania tajemnicy i poufności dotyczącej wszelkich informacji przetwarzanych w toku zatrudnienia w Kancelarii, w tym także po zaprzestaniu wykonywania prac.
4. Zachowania w tajemnicy wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarzania DO w Kancelarii;
5. Niezwłocznego zgłaszania przełożonemu wszelkich naruszeń ochrony DO, jak również wszelkich zaobserwowanych prób lub faktów naruszenia zabezpieczeń pomieszczeń lub systemów informatycznych.

_____
(data i podpis pracownika)

Kraków, dnia 25.05.2018 r.

Załącznik nr 3
Polityka czystego biurka

W Kancelarii Rachunkowej z dniem 25.05.2018 r. wprowadza się Politykę Czystego Biurka (dalej: Polityka CB).

Polityka CB obejmuje wszystkich pracowników oraz współpracowników Kancelarii.

Nadzór nad wykonywaniem Polityki CB powierza się Inspektorowi DO.

Polityka Czystego Biurka

1. Polityka reguluje wymagania oraz procedury ochrony danych poufnych, w tym DO przetwarzanych w Kancelarii przez Pracowników w formie papierowej, w tym:
   1. dokumentów papierowych;
   2. korespondencji listownej;
   3. akt sprawy;
   4. dokumentów źródłowych przekazanych przez Klientów Kancelarii;
   5. korespondencję urzędową.
2. Ilekroć w Polityce CB zostaną wykorzystane następujące definicje i zwroty, należy nadawać im następujące znaczenie:
   1. Polityka CB – oznacza niniejszą Politykę Czystego Biurka wraz ze wszystkimi ewentualnymi załącznikami, która sama w sobie jest częścią Polityka Ochrony DO;
   2. Pracownik – oznacza zarówno każdą osobę fizyczną zatrudnioną w Kancelarii na podstanie umowy o pracę, jak również współpracującą z Kancelarią na podstawie umowy cywilnoprawnej (w tym w zakresie prowadzonej jednoosobowej działalności gospodarczej) oraz studenta lub ucznia niebędących pracownikami Kancelarii w trakcie odbywania praktyk lub stażu zawodowego;
   3. Kancelaria – oznacza właściciel niniejszej Polityki CB
3. Polityka CB obowiązuje wszystkich Pracowników Kancelarii, niezależnie od zajmowanego stanowiska i czasu zatrudnienia w Kancelarii.
4. Każdy Pracownik zobowiązany jest do ograniczenia dostępu osób postronnych do danych poufnych, w tym DO 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 poniższe stosuje się odpowiednio:
   1. 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 DO do zamykanej szuflady lub szafy, celem uniemożliwienia dostępu do dokumentów osobom postronnym.
   2. W przypadku zakończenia przez Pracownika pracy w danym dniu, Pracownik jest obowiązany przed opuszczeniem siedziby Kancelarii do wykonania obowiązku, o którym mowa powyżej oraz do zabezpieczenia dokumentów przed dostępem jakichkolwiek osób postronnych.
      Po zakończonej pracy na biurku mogą znajdować się jedynie telefon stacjonarny i przybory biurowe.
   3. 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, co unormowane jest również w innych przepisach i umowie o pracę.

Kraków, dnia 25.05.2018 r.

Załącznik nr 4
Procedura otwierania i zamykania budynku oraz pomieszczeń biurowych

W Kancelarii Rachunkowej jest wprowadzona w ramach SZJ procedura otwierania i zamykania budynku oraz pomieszczeń biurowych położonych przy ul. Mysłakowskiego 9, w Krakowie, zwaną dalej „Polityką kluczy".

Niniejsza procedura jest uzupełnieniem i uszczegółowieniem Instrukcji ISO z 01.09.2012 roku numer I-18.

Nadzór nad wykonywaniem polityki powierza się Inspektorowi DO oraz Pełnomocnikowi ISO.

Procedura otwierania i zamykania budynków oraz pomieszczeń biurowych

I. Procedura otwierania i przebywania w budynku:

1. Siedzibą Kancelarii Rachunkowej jest lokal biurowy znajdujący się pod ww. adresem, zwany dalej: Lokalem.
2. Lokal skalda się z:
    1. Sekretariatu - ogólnodostępnego dla wszystkich osób w tym m.in. Klientów.
    2. Pomieszczenia roboczego „dużego" na parterze - chronionego kontrolą dostępu.
    3. Pomieszczenia socjalnego na parterze – znajdującego się w strefie chronionej.
    4. Sali konferencyjnej na piętrze - chronionej kontrolą dostępu.
    5. Pomieszczenia socjalnego i kuchni na piętrze – znajdującego się w strefie chronionej.
    6. Pomieszczenia roboczego „małego" na piętrze - chronionego kontrolą dostępu.
    7. Gabinetu Zarządu - chronionego kontrolą dostępu.
    8. Serwerowni - chronionej kontrolą dostępu.
    Serwerownia i Gabinet posiadają szczególny nadzór i nie ma do nich dostępu nikt, bez obecności w środku kogoś z Zarząd Kancelarii.
3. Każdy pracownik ma obowiązek dbania o to by obszary chronione były zamknięte. Każdorazowy dostęp do tych pomieszczeń jest odnotowywany w elektronicznej kontroli dostępu.
4. Karty wydaje za potwierdzeniem i ewidencjonuje na liście kart dostępu Zarząd Kancelarii.
5. Każde przejście przez drzwi do obszaru chronionego wymaga użycia karty elektronicznej.
6. Do otwierania oraz zamykania Lokalu uprawnione są osoby wskazane w Załączniku F-17 ISO.
7. Otwarcia Lokalu i wyłączeniu systemu alarmowego dokonuje osoba uprawniona.
8. Każdy pracownik ma obowiązek logowania się do elektronicznej kontroli dostępu. Terminal A przy pierwszym wejściu, a terminal B przy wyjściu z Kancelarii, za pomocą kartę elektronicznej lub w przypadku zapomnienia tejże kodem PIN.
9. W razie niemożności otwarcia lub zamknięcia budynku lub pomieszczeń biurowych, pracownik niezwłocznie zawiadamia o tym fakcie Zarząd Kancelarii i oczekuje na miejscu do czasu rozwiązania problemu zamknięcia Kancelarii.
10. Przebywanie pracowników w Lokalu po godzinach pracy powyżej 30 minut od zakończenia pracy jest niedozwolone, z zastrzeżeniem:
    1. Przebywanie pracowników w Lokalu po godzinach pracy lub dni wolne od pracy jest dopuszczalne za zgodą wyrażoną e-mailem służbowym.
    2. Od wymogów określonych w powyżej zwolnieni są:
        1. Zarząd Kancelarii.
        2. Personel IT.
        3. inne osoby upoważnione pisemnie przez Zarząd Kancelarii.

II. Procedura włączania i wyłączania systemów alarmowych.

1. Lokal podlega dozorowi i ochronie polegającej na całodobowym monitorowaniu systemu sygnalizacji alarmowo-włamaniowej Satel oraz systemu sygnalizacji pożarowej. Dodatkowo pomieszczenia monitorowane są za pomocą kamer wizyjnych i systemu audio.
2. Dodatkowo po zazbrojeniu systemu alarmowego podlega ochronie i monitorowaniu sygnałów przez firmę ochroniarską Juwentus, na zasadach określonych w Umowie zawartej z tym podmiotem.
3. Uprawnienia do włączenia i wyłączenia centralnego systemu alarmowego posiadają upoważnione osoby, wyszczególnione w Załączniku nr F-17 ISO. Każda z tych osób posługuje się indywidualnym hasłem dostępu. System każdorazowo rejestruje datę, godzinę oraz osobę dokonującą czynności włączenia i wyłączenia alarmu.
4. Osoby posiadające hasła dostępu do systemu alarmowego zobowiązane są do zachowania szczególnej ostrożności w trakcie ich używania. Hasła dostępu stanowią tajemnicę służbową.
5. W przypadku wystąpienia alarmu w Lokalu firma ochroniarska powiadamia Zarząd Kancelarii który podejmuje stosowne działania uzgodnione z firmą ochroniarską.

III. Procedura zamykania budynku i pomieszczeń.

1. Po zakończeniu pracy pracownicy mają obowiązek zamknąć pomieszczenia Kancelarii na klucz zgodnie z Instrukcją I-18 ISO.
2. Włączenie systemu alarmowego następuje po sprawdzeniu pomieszczeń biurowych, korytarzy oraz pomieszczeń sanitarnych znajdujących się w Lokalu i stwierdzeniu możliwość zamknięcia Lokalu.

IV. Procedura przechowywania i dysponowania kluczami.

1. Prowadzona jest ewidencja pobierania i zdawania kluczy, wg. Instrukcji I-18 ISO. Ewidencja przechowywana jest w sekretariacie.
2. Klucze do pomieszczeń biurowych przechowywane są w skrzynce metalowej, z wyłączeniem kluczy do serwerowni i archiwum, przechowywanych przez Zarząd Kancelarii.
3. Osoby dysponujące kluczami zobowiązane są do odpowiedniego zabezpieczenia kluczy przed ich zgubieniem i kradzieżą oraz wpisywania faktu ich pobrania/zdania do ewidencji wejść do Lokalu.
4. W przypadku zagubienia, zaginięcia klucza lub stwierdzenia jego braku pracownik zgłasza ten fakt natychmiast Zarządowi Kancelarii i w razie konieczności wydania kluczy zapasowych składa w tej sprawie wniosek.
5. Zabrania się pracownikom samodzielnego dorabiania kluczy do Lokalu i pomieszczeń biurowych.
6. Zabrania się pozostawiania kluczy w zamkach od drzwi podczas obecności i nieobecności pracownika w pomieszczeniu biurowym.
7. Zabrania się udostępniania kluczy osobom nieupoważnionym.

V. Postanowienia końcowe:

1. Procedura wchodzi w życie z dniem ogłoszenia.

Załącznik nr 5

Rejestr Czynności przetwarzania

Kancelarii Rachunkowej

Administratora Danych: **Faber Sp. z o.o.**

Czynność przetwarzania	**Cel przetwarzania**	**Podstawa przetwarzania**	**Kategorie osób**	**Kategorie danych**	**Kategorie odbiorców**	**Sposób przetwarzania danych**	**Okres przechowywania danych**	**Stosowane środki bezpieczeństwa**
Obsługa stosunku pracy	Zarządzanie personelem, realizacja uprawnień i obowiązków pracodawcy wynikających z Kodeksu pracy	W zakresie danych, o których mowa Kodeksie Pracy: Umowa o pracę. W pozostałym zakresie – zgoda pracownika	Pracownicy Kancelarii zatrudnieni w Kancelarii na podstawie stosunku pracy	Imię, nazwisko, data urodzenia, PESEL, numer telefonu pracownika, mail służbowy i prywatny, miejsce zamieszkania	Zarząd Kancelarii, pracownicy kancelarii,	papierowo oraz elektronicznie	Czas trwania stosunku pracy oraz okres archiwizacji i przechowywania dokumentów pracowniczych wymagany przepisami prawa	

Kraków, dnia …..... r.

Załącznik nr 6
Wzór zgłoszenia naruszenia ochrony DO

Prezes Urzędu Ochrony DO

Zgłoszenie naruszenia ochrony DO

Działając w imieniu i na rzecz Kancelarii Rachunkowej siedzibą w Krakowie 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 DO 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 DO:

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

Załącznik nr 7

Rejestr naruszeń ochrony DO

Kancelarii Rachunkowej

Administratora Danych: **Faber Sp. z o.o.**

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