



*Załącznik nr 1 do uchwały nr 2/ 2022
ZARZĄDU ECOEN CONSULT Sp. z o.o.
z dnia 27 czerwca 2022 r.*

Polityka ochrony danych osobowych w ECOEN CONSULT Sp. z o.o.

Pyrzowice, dnia 27.06.2022 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 firmie ECOEN CONSULT Sp. z o.o. 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; Zarząd ECOEN CONSULT Sp. z o.o. zapewnia, że domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

§ 1.

Postanowienia wstępne

1. Polityka określa zasady przetwarzania oraz zabezpieczania danych osobowych w firmie ECOEN CONSULT Sp. z o.o., 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 firmie wymogów, procedur oraz zasad ochrony danych osobowych. Polityka zawiera:
 - a. opis zasad ochrony danych obowiązujących w firmie;
 - b. zbiór procedur, instrukcji i regulacji szczegółowych dotyczących przetwarzania danych osobowych w firmie, dotyczących poszczególnych obszarów z zakresu ochrony danych osobowych, stanowiących załączniki do Polityki.
2. Polityka obowiązuje wszystkich członków Zarządu, pracowników oraz współpracowników firmy ECOEN CONSULT Sp. z o.o. Za przestrzeganie i utrzymanie postanowień Polityki odpowiedzialni są:
 - a. Zarząd ECOEN CONSULT Sp. z o.o.;
 - b. Zewnętrzna księgowość.
3. Dla skutecznej realizacji Polityki, uwzględniając zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia firma ECOEN CONSULT Sp. z o.o. zapewnia:
 - a. wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania danych osobowych z wymogami prawa oraz niezbędne zabezpieczenie przetwarzanych danych osobowych;
 - b. stałe monitorowanie zgodności przetwarzania danych osobowych z wymogami prawa oraz poddawanie środków, o których mowa w ust. 3 pkt. a ciągłym przeglądom oraz uaktualnianiu;
 - c. kontrolę i nadzór nad przetwarzaniem danych osobowych.
4. Nadzór nad przestrzeganiem postanowień polityki zapewnia Zarząd ECOEN CONSULT Sp. z o.o. Nadzór, o którym mowa w zdaniu poprzedzającym zmierza w szczególności, ale nie wyłącznie do zapewnienia, że czynności związane z przetwarzaniem danych osobowych w firmie ECOEN CONSULT Sp. z o.o. są zgodne z wymogami prawa oraz postanowieniami Polityki.

5. Zarząd ECOEN CONSULT Sp. z o.o. zapewnia zgodność postępowania kontrahentów, w tym w szczególności podmiotów przetwarzających z postanowieniami Polityki w odpowiednim zakresie we wszystkich sytuacjach, w których dochodzi do przekazania tym podmiotom danych osobowych do przetwarzania, w tym przechowywania.
6. Polityka jest przechowywana i udostępniana w wersji papierowej oraz elektronicznej w siedzibie firmy ECOEN CONSULT Sp. z o.o. w Pyrzowicach przy ul. Centralnej 5, 42-625 Ożarówice.
7. Politykę udostępnia się:
 - a. obligatoryjnie wszystkim osobom upoważnionym do przetwarzania danych osobowych, celem zapewnienia osobom upoważnionym należytej wiedzy oraz informacji na temat zasad i wymogów dotyczących przetwarzania danych osobowych;
 - b. osobom zainteresowanym, w szczególności osobom fizycznym, których dane dotyczą – na ich wniosek.

§ 2.

Słownik pojęć

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

Polityka – oznacza niniejszą Politykę wraz ze wszystkimi ewentualnymi Załącznikami;

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;

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);

Osoba upoważniona – oznacza osobę upoważnioną przez firmę do przetwarzania danych osobowych w danym zakresie;

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;

Zbiór danych – oznacza każdy uporządkowany zestaw danych osobowych, dostępny według określonych kryteriów;

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ECOEN CONSULT Sp. z o.o. (usługodawca, zewnętrzna księgowość);

Rejestr - oznacza Rejestr czynności przetwarzania danych osobowych firmy;

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

Firma – ECOEN CONSULT Sp. z o.o.

Pracownicy – oznaczają zarówno osoby zatrudnione w firmie na podstawie stosunku pracy, jak również osoby fizyczne współpracujące z firmą na podstawie Umowy cywilnoprawnej;

System – oznacza System ochrony danych osobowych w firmie, o którym mowa w niniejszej Polityce;

Dane wrażliwe – oznaczają dane osobowe, o których mowa w art. 9 RODO.

§ 3.

Dane osobowe

1. Firma przetwarza Dane osobowe gromadzone w zbiorach danych. Zbiory danych przetwarzane w Firmie określa Załącznik nr 1 do Polityki.
2. Uaktualnienie lub poszerzenie listy zbiorów danych następuje po uprzednim przeprowadzeniu analizy skutków oraz ryzyka przetwarzania danych osobowych dla praw i wolności osób fizycznych objętych zbiorem.
3. Firma 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 firma obligatoryjnie przeprowadza uprzednią ocenę skutków przetwarzania, o których mowa w art. 35 RODO.
4. Dane osobowe domyślnie przetwarzane są na obszarze obejmującym pomieszczenia biurowe firmy zlokalizowane w Pyrzowicach przy ul. Centralnej 5, 42- 625 Ożarówice (pomieszczenia o nr 113 i 114). 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

1. Firma 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 dane osobowe przetwarzane w firmie zobowiązane są do przetwarzania danych osobowych zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych wewnętrznych aktów prawnych firmy lub procedur wewnętrznych związanych z przetwarzaniem danych osobowych.

3. Przy zatrudnianiu pracowników oraz w toku zatrudnienia firma zapewnia, że:
 - a. pracownicy przed przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad przetwarzania i ochrony danych osobowych.
 - b. każdy z pracowników zostaje upoważniony na piśmie do przetwarzania danych osobowych w niezbędnym zakresie, zgodnie ze wzorem stanowiącym Załącznik nr 2 do Polityki;
 - c. każdy z pracowników zostaje zobowiązany do zachowania poufności i integralności danych osobowych, zgodnie ze wzorem stanowiącym Załącznik nr 3 do Polityki, przy czym pracownicy zobowiązani są w szczególności, ale nie wyłącznie do:
 - ścisłego przestrzegania zakresu upoważnienia;
 - przestrzegania wymogów prawa oraz postanowień Polityki w zakresie przetwarzania;
 - zachowania w tajemnicy danych osobowych;
 - zachowania w tajemnicy, zachowania poufności i integralności danych osobowych;
 - niezwłocznego zgłaszania firmie wszelkich incydentów związanych z naruszeniem bezpieczeństwa danych osobowych.
4. Firma zapewnia, aby dane osobowe przetwarzane w firmie były:
 - a. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
 - b. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
 - c. adekwatne, stosowne oraz ograniczone do tego, co niezbędne; do celów, w których są przetwarzane;
 - d. 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");
 - e. 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;
 - f. 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.
5. Przy zapewnieniu przetwarzania danych osobowych zgodnie z zasadami wskazanymi w ust.1 firma opiera przetwarzanie na następujących podstawach:
 - a. **Legalność** – dba o ochronę prywatności i przetwarza dane osobowe zgodnie z wymogami prawa;
 - b. **Bezpieczeństwo** – zapewnia odpowiedni poziom bezpieczeństwa danych osobowych podejmując stale działania w tym zakresie;
 - c. **Prawa Jednostki** – umożliwia osobom, których dane osobowe są przetwarzane, wykonywanie swoich praw i prawa te realizuje;

- d. **Rozliczalność** –zapewnia należyte udokumentowanie sposobu spełniania obowiązków w zakresie ochrony danych osobowych.
6. Firma 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

Firma 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:

- a. 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;
- b. zamykanie pomieszczeń tworzących obszar, o którym mowa w § 3 ust. 4 Polityki na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osobom trzecim;
- c. zapewnienie zabezpieczenia obszaru, o którym mowa w § 3 ust. 4 Polityki przed czynnikami losowymi, takimi jak pożar lub powódź;
- d. wykorzystywanie zamkniętych szafek, szuflad lub innych środków technicznych uniemożliwiających osobom niepowołanym dostęp do przechowywanych w nich danych osobowych;
- e. wdrożenie Polityki czystego biurka, która stanowi Załącznik nr 4 do Polityki;
- f. wdrożenie Procedury otwierania i zamykania pomieszczeń biurowych, która stanowi Załącznik nr 5 do Polityki;
- g. zapewnienie skutecznego usuwania lub niszczenia dokumentów zawierających dane osobowe, w sposób uniemożliwiający ich późniejsze odtworzenie;
- h. zapewnienie bezpieczeństwa sprzętowego i informatycznego, obejmującego:
- ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz,
 - zapewnienie aktualności stosowanego oprogramowania,
 - zabezpieczenie sprzętu komputerowego wykorzystywanego w firmie przed złośliwym oprogramowaniem,
 - zapewnienie stałego i częstotliwego sporządzania kopii zapasowych danych przechowywanych na komputerach, serwerze oraz w sieci firmy,

- ograniczenie dostępu do sprzętu komputerowego, serwera oraz sieci lokalnej poprzez stosowanie reguł uwierzytelniania;
- i. przeprowadzanie analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
- j. realizację standardów weryfikacji i doboru podmiotów przetwarzających, jak również warunków powierzenia przetwarzania danych na rzecz poszczególnych podmiotów przetwarzających;
- k. monitorowanie zmian w zakresie procesów przetwarzania danych osobowych w firmie oraz na bieżąco zarządza zmianami mającymi wpływ na ochronę danych osobowych w firmie.

§ 6.

Rejestr czynności przetwarzania danych osobowych

1. Rejestr obejmuje kategorie czynności przetwarzania danych osobowych. Za pośrednictwem Rejestru firma dokumentuje czynności przetwarzania danych osobowych oraz inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Rejestr stanowi Załącznik nr 6 do Polityki.
2. Za pośrednictwem Rejestru, w szczególności poprzez wskazanie w Rejestrze ogólnych środków ochrony danych osobowych objętych wyodrębnioną czynnością przetwarzania, firma dąży również do wykazania zgodności przetwarzania danych osobowych z wymogami prawa.
3. W Rejestrze, odrębnie dla każdej zidentyfikowanej kategorii czynności przetwarzania danych osobowych, odnotowuje się co najmniej:
 - a. nazwę zbioru;
 - b. cel przetwarzania;
 - e. podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu firmy, jeśli podstawą przetwarzania jest uzasadniony interes;
 - f. opis kategorii osób, których dane osobowe przetwarzane są w ramach danej czynności;
 - g. opis kategorii danych osobowych przetwarzanych w ramach danej czynności;
 - f. opis kategorii odbiorców danych, w tym podmiotów przetwarzających;
 - g. informację o ewentualnym przekazaniu danych osobowych poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;
 - h. ogólny opis technicznych i organizacyjnych środków ochrony danych osobowych, znajdujących zastosowanie do danej czynności.
4. W przypadku uaktualnienia lub poszerzenia kategorii czynności przetwarzania danych osobowych, firma dokonuje niezwłocznego uaktualnienia Rejestru celem zapewnienia zgodności Rejestru ze stanem faktycznym oraz zakresem operacji przetwarzania danych osobowych w firmie.

5. Postanowienia § 6 ust. 3 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. Firma 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 firmę, uzasadniony cel firmy.

§ 7.

Realizacja obowiązków wobec osób, których dane osobowe dotyczą

1. Firma 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.
2. Firma dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane osobowe przetwarza.
3. Firma publikuje na stronie internetowej firmy oraz pozostawia do wglądu w siedzibie firmy:
 - a. Politykę;
 - b. Informację o prawach osób, których dane dotyczą;
 - c. Informację o zakresie przetwarzanych danych osobowych w poszczególnych celach;
 - d. Metodach kontaktu z firmą w zakresie danych osobowych;
4. W celu realizacji praw osoby, której dane osobowe dotyczą firma zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez firmę, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.
5. Firma dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób, informując osobę, której dane dotyczą:
 - a. o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
 - b. o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej;
 - c. o planowanej zmianie celu przetwarzania danych;
 - d. przed uchycieniem ograniczenia przetwarzania;
 - e. o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe);
 - f. o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

6. Firma bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
7. Niezależnie od postanowień ust. 5, firma określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu Biurowca Małej i Średniej Przedsiębiorczości monitoringiem wizyjnym).
8. Na żądanie osoby dotyczące dostępu do jej danych, firma 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.
9. Firma wydaje osobie, której dane osobowe dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.
10. Firma dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której dane osobowe dotyczą. Firma 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.
11. Firma uzupełnia i aktualizuje dane na żądanie osoby, której dane osobowe dotyczą. Firma ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Firma może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez firmę procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
12. Z uwzględnieniem ust. 13, na żądanie osoby, firma usuwa dane, gdy:
 - a. dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
 - b. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
 - c. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
 - d. dane były przetwarzane niezgodnie z prawem,
 - e. konieczność usunięcia wynika z obowiązku prawnego,
 - f. żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
13. Firma 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.
14. Jeżeli dane podlegające usunięciu zostały upublicznione przez firmę, firma 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 firma informuje osobę o odbiorcach danych, na żądanie tej osoby.
15. Firma dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
 - a. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

- b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
 - c. firma nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
 - d. osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie firmy zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
16. W trakcie ograniczenia przetwarzania firma 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. Firma informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych firma informuje osobę o odbiorcach danych, na żądanie tej osoby.
17. Na żądanie osoby firma 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 firmie, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych firmy.
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 firmę w oparciu o uzasadniony interes firmy lub o powierzone firmie zadanie w interesie publicznym, firma zobowiązuje się uwzględnić sprzeciw, o ile nie zachodzą po stronie firmy ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
19. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez firmę na potrzeby marketingu bezpośredniego, firma uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

§ 8.

Minimalizacja danych

1. Firma wdraża procedury służące realizacji zasady minimalizacji przetwarzanych danych osobowych pod względem:
- a. adekwatności danych osobowych do celów przetwarzania, obejmujących ograniczenie ilości przetwarzanych danych osobowych oraz zakresu przetwarzania do celu przetwarzania;
 - b. ograniczenia dostępu do danych osobowych wyłącznie do osób upoważnionych, dla których wykorzystanie danych osobowych w określonym zakresie jest niezbędne dla prawidłowej realizacji obowiązków;

- c. ograniczenia czasu przechowywania danych osobowych do okresu, dla którego przechowywanie danych osobowych jest niezbędne ze względu na realizację celu przetwarzania lub obowiązków nałożonych na firmę.
2. Firma dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
3. Firma stosuje ograniczenia dostępu do danych osobowych poprzez wdrożenie:
 - a. zobowiązania pracowników do zachowania poufności, w tym w zakresie danych osobowych;
 - b. weryfikację kręgu wewnętrznych odbiorców danych osobowych poprzez nadawanie poszczególnym pracownikom szczegółowych upoważnień co do przetwarzania danych osobowych;
 - c. wdrożenie logicznych środków technicznych ochrony danych osobowych poprzez ograniczenie dostępu do systemów, oprogramowania oraz zasobów sieciowych wykorzystywanych w procesie przetwarzania danych osobowych;
 - d. wdrożenie fizycznych środków technicznych ochrony danych osobowych.
4. Firma dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających. Firma 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 firmy.
6. Firma przetwarza dane osobowe z uwzględnieniem kryteriów wskazanych w Rejestrze. Firma wdraża mechanizmy kontroli cyklu życia danych osobowych w firmie, 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 firmy, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez firmę. 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

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, firma wdraża środki techniczne i organizacyjne zapewniające należyty stopień ochrony danych osobowych, odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez firmę.

2. Firma przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
 - a. firma kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;
 - b. firma przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Firma 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;
3. Firma 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

1. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności, ale nie wyłącznie:
 - a. naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe;
 - b. udostępnienie danych osobowych osobom nieupoważnionym;
 - c. przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich przetwarzania;
 - d. nieuprawnione lub przypadkowe uszkodzenie, utratę, zniszczenie lub zmianę danych osobowych.
2. W przypadku stwierdzenia naruszenia ochrony danych osobowych firma dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych oraz szacuje skalę ryzyka.
3. W przypadku naruszenia ochrony danych osobowych, firma bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorcemu 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 7 do Polityki.
4. Jeżeli ryzyko naruszenia praw i wolności osoby, której dane osobowe dotyczą jest wysokie, firma zawiadamia o incydencie także osobę, której dane dotyczą, chyba że:
 - a. firma wdroży odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

- b. firma zastosuje następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; lub
 - c. 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 skutecznym sposób.
5. Niezależnie od obowiązków wskazanych w ust. 2- 4, firma 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 8 do Polityki.

§ 11.

Powierzenie przetwarzania

- 1. Firma 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.
- 2. Firma 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, firma 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

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

§ 13.

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 wchodzi w życie nie wcześniej niż w terminie 7 dni od dnia ich ogłoszenia.
4. Do Polityki dołączono następujące Załączniki, stanowiące integralną część Polityki:
 - Załącznik nr 1 – Lista zbiorów danych w firmie;
 - Załącznik nr 2 – Wzór upoważnienia do przetwarzania danych osobowych;
 - Załącznik nr 3 – Wzór zobowiązania do zachowania poufności;
 - Załącznik nr 4 – Polityka czystego biurka;
 - Załącznik nr 5 – Procedura otwierania i zamykania pomieszczeń biurowych;
 - Załącznik nr 6 – Wzór rejestru czynności przetwarzania;
 - Załącznik nr 7 – Wzór zgłoszenia naruszenia ochrony danych osobowych;
 - Załącznik nr 8 – Wzór rejestru naruszeń danych osobowych.

Załącznik nr 1 – Lista zbiorów danych w firmie

Lista zbiorów danych w firmie

Uwzględniając definicję z art. 4 pkt 6 RODO, firma przetwarza dane osobowe zgrupowane w następujących zbiorach danych:

Kandydaci do pracy- obejmujący dane osobowe osób fizycznych ubiegających się o pracę w firmie;

Pracownicy- obejmujący dane osobowe osób fizycznych zatrudnionych w firmie na podstawie stosunku pracy (niezależnie od podstawy jego nawiązania), oraz dane osobowe praktykantów i stażystów firmy;

Umowy cywilnoprawne - obejmujący dane osobowe osób fizycznych współpracujących z firmą na podstawie umowy cywilnoprawnej (umowy zlecenie, umowy o dzieło);

Klienci – obejmujący dane osobowe klientów firmy będących osobami fizycznymi, w tym prowadzącymi jednoosobową działalność gospodarczą, jak również dane osobowe osób fizycznych będących przedstawicielami (reprezentantami) klientów firmy (współwłaściciele, księgowość zewnętrzna, pełnomocnicy osób prawnych, pracownicy klientów występujący w ich imieniu);

Wykonawcy usług- obejmujący dane osobowe wykonawców usług będących osobami fizycznymi prowadzącymi jednoosobową działalność gospodarczą, jak również dane osobowe osób fizycznych będących przedstawicielami (reprezentantami) wykonawców usług (współwłaściciele, księgowość zewnętrzna, pełnomocnicy osób prawnych, pracownicy wykonawców);

Uczestnicy projektów- osoba fizyczna, bezpośrednio korzystająca ze wsparcia w ramach projektu tj. osoba, która spełnia kryteria kwalifikowalności uprawniające do udziału w projekcie zgodnie z zasadami określonymi w Regulaminie rekrutacji i uczestnictwa w projekcie;

Rejestr poczty wychodzącej / przychodzącej- obejmujący dane osobowe osób fizycznych, do których wysyłane i od których odbierane są wiadomości za pomocą służbowej poczty elektronicznej znajdującej się na serwerze ecoen.nazwa.pl;

Konsultacje społeczne- obejmujący dane osobowe osób fizycznych, biorących udział w konsultacjach społecznych zleconych do przeprowadzenia przez klientów firmy.

Załącznik nr 2 – Upoważnienia do przetwarzania danych osobowych

Pyrzowice, dnia r.

Pracownik: Imię i Nazwisko

Upoważnienie pracownika do przetwarzania danych osobowych

Działając w imieniu ECOEN CONSULT Sp. z o.o., 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:.....

zatrudnionemu na stanowisku:

upoważnienie do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych w zakresie : bez ograniczeń.

Upoważnienie obejmuje przetwarzanie danych osobowych:

1. przetwarzanych na nośnikach papierowych;
2. przetwarzanych w systemach informatycznych:
[•],
[•];
3. Dane osobowe objęte zbiorami danych:
[•],
[•].

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 10.05.2018r. 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 3 – Wzór zobowiązania do zachowania poufności

Pyrzowice, dnia r.

Pracownik: Imię i Nazwisko

Zobowiązanie do zachowania poufności

Oświadczam, że w związku z wykonywaniem obowiązków służbowych na rzecz ECOEN CONSULT Sp. z o.o. oraz udzielonym mi upoważnieniem do przetwarzania danych osobowych:

1. zostałem/am poinformowany/a o zasadach przetwarzania i ochrony danych osobowych w ECOEN CONSULT Sp. z o.o., w tym o:
 - a. treści Polityki ochrony danych osobowych;
 - b. procedurach oraz regulacjach dotyczących ochrony danych osobowych obowiązujących w firmie, w tym:
 - c. Polityką czystego biurka;
 - 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);
2. treści informacji oraz regulacji, o których mowa w pkt 1, 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 danych osobowych;
2. zapewnienia ochrony, poufności oraz integralności danych osobowych przetwarzanych w zbiorach przez firmę, 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;
3. zachowania tajemnicy i poufności dotyczącej wszelkich informacji przetwarzanych w toku zatrudnienia w firmie, w tym także po zaprzestaniu wykonywania prac;
4. zachowania w tajemnicy wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych w firmie;
5. 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 4 – Polityka czystego biurka

W ECOEN CONSULT Sp. z o.o. wprowadza się Politykę czystego biurka. Polityka obejmuje wszystkich pracowników oraz współpracowników firmy.

Nadzór nad wykonywaniem polityki powierza się Zarządowi Spółki.

Polityka czystego biurka

1. Polityka reguluje wymagania oraz procedury ochrony danych poufnych, w tym danych osobowych przetwarzanych w ECOEN CONSULT Sp. z o.o. przez pracowników w formie papierowej, w tym:
 - a. dokumentów papierowych;
 - b. korespondencji listownej;
 - c. akt sprawy;
 - d. dokumentów źródłowych przekazanych przez klientów firmy;
 - 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 firmie na podstawie umowy o pracę, jak również współpracującą z firmą na podstawie umowy cywilnoprawnej (w tym w zakresie prowadzonej jednoosobowej działalności gospodarczej) oraz studenta lub ucznia niebędących pracownikami firmy w trakcie odbywania praktyk lub stażu zawodowego;
 - c. **Firma** – oznacza ECOEN CONSULT Sp. z o.o.
3. Polityka obowiązuje wszystkich pracowników firmy, niezależnie od zajmowanego stanowiska i czasu zatrudnienia w firmie.
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 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 firmy do wykonania obowiązku, o którym mowa w ust. 6 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, 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 firmie, jak również w sytuacjach określonych w Polityce ochrony danych osobowych, 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 nie przewiduje innego sposobu zadysponowania dokumentów lub nie nakazuje jego pozostawienia lub archiwizacji.

Załącznik nr 5 – Procedura otwierania i zamykania pomieszczeń biurowych

W ECOEN CONSULT Sp. z o.o. wprowadza się procedurę otwierania i zamykania pomieszczeń biurowych o nr 113 i 114, zlokalizowanych w Biurowcu Małej i Średniej Przedsiębiorczości w Pyrzowicach przy ul. Centralnej 5, zwaną dalej „Polityką kluczy”.

Nadzór nad wykonywaniem polityki powierza się Zarządowi Spółki.

Procedura otwierania i zamykania pomieszczeń biurowych

1. Procedura otwierania i przebywania w Lokalu

- a. Siedziba ECOEN CONSULT Sp. z o.o. znajduje się w Pyrzowicach przy ul. Centralnej 5 w Biurowcu Małej i Średniej Przedsiębiorczości. Biura firmy znajdują się w pomieszczeniach o nr 113 i 114 i zwane są dalej: Lokalem.
- b. Do otwierania oraz zamykania Lokalu uprawnione są osoby wskazane w Załączniku nr 1 do Procedury.
- c. W przypadku nieobecności osób posiadających klucze główne do Lokalu, Zarząd Spółki może upoważnić innego pracownika do otwierania i zamykania Lokalu.
- d. W razie niemożności otwarcia lub zamknięcia Lokalu, pracownik niezwłocznie zawiadamia o tym fakcie Zarząd Spółki.
- e. W pomieszczeniach biurowych, podczas godzin pracy, gdzie przebywa tylko jeden pracownik, jest on zobowiązany do każdorazowego zamknięcia pomieszczenia w przypadku jego opuszczenia.
- f. Przebywanie pracowników w Lokalu po godzinach pracy powyżej 30 minut od zakończenia pracy jest niedozwolone, z zastrzeżeniem lit. g oraz h.
- g. Przebywanie pracowników w Lokalu po godzinach pracy lub w dni wolne od pracy jest dopuszczalne za zgodą wyrażoną na piśmie lub na podstawie pisemnego polecenia służbowego Zarządu Spółki, a w razie jego nieobecności osoby go zastępującej.
- h. Od wymogów określonych w lit. f wyżej zwolnieni są:
 - 1) Zarząd Spółki,
 - 2) inne osoby upoważnione pisemnie przez Zarząd Spółki.

2. Procedura zamykania pomieszczeń.

- a. Po zakończeniu pracy pracownicy wymienieni w Załączniku nr 1 mają obowiązek zamknąć Lokal na klucz.
- b. Po zakończeniu pracy osoby wymienione w Załączniku nr 1 do Procedury mają obowiązek przekazać klucze pracownikowi recepcji Biurowca Małej i Średniej Przedsiębiorczości w Pyrzowicach.

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

3. Procedura przechowywania i dysponowania kluczami.

- a. W Załączniku nr 1 wymieniono osoby dysponujące kluczami do lokalu w godzinach pracy firmy.
- b. Osoby dysponujące kluczami zobowiązane są do odpowiedniego zabezpieczenia kluczy przed ich zgubieniem i kradzieżą.
- c. W przypadku zagubienia, zaginięcia klucza lub stwierdzenia jego braku pracownik zgłasza ten fakt natychmiast Zarządowi Spółki i pracownikowi recepcji Biurowca Małej i Średniej Przedsiębiorczości w Pyrzowicach i w razie konieczności wydania kluczy zapasowych (z sejf), za zgodą Zarządu Spółki, wnioskuje o ich wydanie do pracownika recepcji Biurowca Małej i Średniej Przedsiębiorczości w Pyrzowicach.
- d. Wydawanie kluczy zapasowych (z sejf) pracownikowi firmy przez pracownika recepcji Biurowca Małej i Średniej Przedsiębiorczości w Pyrzowicach może odbywać tylko w uzasadnionych sytuacjach.
- e. Zabrania się pracownikom samodzielnego dorabiania kluczy do Lokalu.
- f. Zabrania się pozostawiania kluczy w zamkach od drzwi podczas obecności i nieobecności pracownika w pomieszczeniu biurowym.
- g. Zabrania się udostępniania kluczy osobom nieupoważnionym.

4. Upoważnienia

Osoby wyszczególnione w Załączniku nr 1 do Procedury otrzymują stosowne upoważnienia do otwierania i zamykania Lokalu. Wzór upoważnienia stanowi Załącznik nr 2 do Procedury.

5. Postanowienia końcowe

Do Procedury dołączono następujące Załączniki:

- 1) Załącznik nr 1 – Wzór wykazu osób uprawnionych do otwierania i zamykania pomieszczeń;
- 2) Załącznik nr 2 – Wzór upoważnienia do otwierania i zamykania pomieszczeń;

Załącznik nr 1 do Procedury otwierania i zamykania pomieszczeń biurowych

Wykaz osób uprawnionych do otwierania i zamykania pomieszczeń

Część 1 Wykaz osób stale uprawnionych do otwierania i zamykania Lokalu

Następujące osoby posiadają **stały dostęp** do Lokalu:

1.
2.

Część 2 Wykaz osób czasowo uprawnionych do otwierania i zamykania Lokalu

Następujące osoby posiadają **czasowy dostęp** do Lokalu:

1.
2.

Załącznik nr 2 do Procedury otwierania i zamykania oraz pomieszczeń biurowych

Pyrzowice, dnia

Upoważnienie do otwierania i zamykania pomieszczeń

Działając w imieniu ECOEN CONSULT Sp. z o.o. niniejszym upoważniam pracownika: Imię i Nazwisko do stałego/czasowego otwierania i zamykania Lokalu kluczami w ilości 1 komplet składający się z dwóch kluczy (po jednym kluczu do pomieszczenia biurowego nr 113 i 114).

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

[Data i podpis Członka Zarządu Spółki]

Niniejszym potwierdzam zapoznanie się z treścią upoważnienia oraz zobowiązania.

[Data i podpis pracownika]



Załącznik nr 6 – Rejestr czynności przetwarzania

Rejestr czynności przetwarzania w ECOEN CONSULT Sp. z o.o.

Dane Administratora Danych: ECOEN CONSULT Sp. z o.o., Pyrzowice, ul. Centralna 5, 42- 625 Ożarówce, NIP 645-25-36-127, tel. +48 609-852-366

Nazwa zbioru	Cel przetwarzania	Podstawa przetwarzania	Osoby, których dane dotyczą	Kategorie przetwarzanych danych	Kategorie odbiorców	Sposób przetwarzania danych	Okres przechowywania danych	Stosowane środki bezpieczeństwa

Załącznik nr 7 - Zgłoszenia naruszenia ochrony danych osobowych

Pyrzowice, dnia

ECOEN CONSULT Sp. z o.o.

Pyrzowice, ul. Centralna 5

42- 625 Ożarówice

Prezes Urzędu Ochrony Danych Osobowych
[Adres organu]

Zgłoszenie naruszenia ochrony danych osobowych

Działając w imieniu firmy ECOEN CONSULT Sp. z o.o. z siedzibą w Pyrzowicach przy ul. Centralnej 5, 42-625 Ożarówice, 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 8 – Rejestr naruszeń ochrony danych osobowych

Rejestr 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 zmniejszenia jego negatywnych skutków	Rezultat działań naprawczych