POLITYKA OCHRONY DANYCH OSOBOWYCH

1. Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych” (dalej: Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Kursy Maturalne Potęga Wiedzy (dalej: Firma).

   Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).

2. Polityka zawiera:

   2.1. opis zasad ochrony danych obowiązujących w Firmie;

   2.2. instrukcje zarządzania systemami informatycznymi;

   2.3. odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);

   2.4. informacje w sprawie monitoringu, stanowiącą załącznik nr 8 do niniejszego dokumentu;

   2.5. zasady czystego biurka, stanowiące załącznik nr 9 do niniejszego dokumentu.

3. Skróty i definicje:

   3.1. Administrator danych osobowych (ADO) – Joanna Bujak prowadząca działalność gospodarczą pod firmą Kursy Maturalne Potęga Wiedzy;

   3.2. Administrator systemów informatycznych (ASI) – Joanna Bujak prowadząca działalność gospodarczą pod firmą Kursy Maturalne Potęga Wiedzy, realizująca zadania o charakterze technicznym, związane z bieżącym utrzymaniem systemów informatycznych;

   3.3. Dane – oznacza dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu;

   3.4. Dane szczególnych kategorii – oznacza dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;

   3.5. Firma – oznacza Kursy Maturalne Potęga Wiedzy prowadzone przy ul. Marii Rodziewiczówny1/476, w 04-187 Warszawa;

   3.6. Hasło – oznacza ciąg znaków literowych, cyfrowych, literowo – cyfrowych lub innych, znany jedynie użytkownikowi (systemu informatycznego);

3.7. Kopia bezpieczeństwa – oznacza kopię danych systemu informatycznego wykonaną na elektronicznym nośniku zewnętrznym (np. pendrive) w celu zapewnienia możliwości odtworzenia systemu wraz z danymi w wypadku ich utraty lub uszkodzenia infrastruktury techniczno – systemowej;

3.8. Osoba – oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;

3.9. Osoba upoważniona – oznacza osobę posiadającą upoważnienie i dopuszczoną do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu, w tym też jako użytkownik;

3.10. Polityka – oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, przetwarzania, ochrony i dystrybucji danych w Firmie;

3.11. Profilowanie – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań wiarygodności, zachowania, lokalizacji lub przemieszczania się;

3.12. Przetwarzanie danych osobowych – oznacza operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie, udostępnianie, dopasowywanie, łączenie, ograniczanie, usuwanie, niszczenie;

3.13. RODO – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1);

3.14. RCPD lub Rejestr – oznacza Rejestr Czynności Przetwarzania Danych Osobowych;

3.15. System – oznacza system informatyczny, czyli zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

3.16. Użytkownik – oznacza osobę dopuszczoną do pracy w systemie informatycznym, posługującą się hasłem lub innym atrybutem w celu potwierdzenia swojej autentyczności.

4. Do podstawowych zadań Administratora danych osobowych należy:

4.1. wdrażanie odpowiednich środków technicznych i organizacyjnych w celu skutecznej realizacji zasad ochrony danych i w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak aby spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą;

4.2. wdrażanie odpowiednich środków technicznych i organizacyjnych, by domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania;

4.3. poprzez proces zarządzania ryzykiem prowadzenie systematycznej oceny, czy stopień bezpieczeństwa jest odpowiedni;

4.4. stworzenie warunków, aby przetwarzanie danych osobowych było zgodne z podstawowymi zasadami określonymi w RODO;

4.5. zapewnienie wykonywania obowiązków, które wynikają z praw osób, których dotyczą przetwarzane dane osobowe;

4.6. zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych;

4.7. nadawanie, modyfikowanie i odwoływanie upoważnień osób do przetwarzania danych osobowych w powierzonych systemach/zbiorach, zgodnie ze wzorem stanowiącym załącznik nr 6 do niniejszego dokumentu;

4.8. prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych, zgodnie ze wzorem, który stanowi załącznik nr 7 do niniejszego dokumentu.

5. Do podstawowych zadań Administratora systemów informatycznych należy:

5.1. bieżące utrzymywanie i modernizacja infrastruktury techniczno – systemowej;

5.2. rejestrowanie i wyrejestrowywanie użytkowników systemu;

5.3. przydzielanie uprawnień;

5.4. określenie trybu i częstotliwości zmiany haseł i reguł ich tworzenia;

5.5. wykonywanie procedury kopii bezpieczeństwa oraz ich właściwe przechowywanie, sprawdzanie poprawności zapisu i ich niszczenie;

5.6. wdrożenie stosownych procedur w sytuacji naruszenia ochrony danych osobowych;

5.7. przeprowadzanie szkoleń osób przewidzianych do realizowanie zadań związanych z przetwarzaniem danych osobowych z zakresu ochrony danych osobowych przetwarzanych w formie elektronicznej z wykorzystaniem systemu informatycznego.

6. Ochrona Danych Osobowych w Firmie – zasady ogólne

6.1. Filary ochrony danych osobowych w Firmie:

6.1.1. legalność – Firma dba o ochronę prywatności i przetwarza dane zgodnie z prawem;

6.1.2. bezpieczeństwo – Firma zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie;

6.1.3. prawa jednostki – Firma umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje;

6.1.4. rozliczalność – Firma dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

6.2. Zasady ochrony danych. Firma przetwarza dane osobowe z poszanowaniem następujących zasad:

6.2.1. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

6.2.2. rzetelnie i uczciwie (rzetelność);

6.2.3. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

6.2.4. w konkretnych celach i nie „na zapas” (minimalizacja);

6.2.5. nie więcej niż potrzeba (adekwatność);

6.2.6. z dbałością o prawidłowość danych (prawidłowość);

6.2.7. nie dłużej niż potrzeba (czasowość);

6.2.8. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

6.3. System ochrony danych. System ochrony danych osobowych w Firmie składa się z następujących elementów:

6.3.1. Rejestr. Firma opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w Firmie; Rejestr budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe; Rejestr osób upoważnionych do przetwarzania danych osobowych. Rejestry są narzędziem rozliczania zgodności z ochroną danych w Firmie.

6.3.2. Podstawy prawne. Firma zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

6.3.2.1. utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość;

6.3.2.2. inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Firma przetwarza dane na podstawie uzasadnionego interesu Firmy.

6.3.3. Obsługa praw jednostki. Firma spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

6.3.3.1. obowiązki informacyjne. Firma przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, ADO lub osoby działające z jego upoważnienia, podczas pozyskiwania danych

osobowych podają jej informacje, zgodnie ze wzorem stanowiącym załącznik nr 3 do niniejszego dokumentu. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, osoba ta otrzymuje informacje zgodnie ze wzorem stanowiącym załącznik nr 4 do niniejszego dokumentu;

6.3.3.2. możliwość wykonania żądań. Firma weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania osób tak, aby były realizowane w terminach i w sposób wymagany przez RODO i udokumentowane;

6.3.3.3. zawiadamianie o naruszeniach. Firma stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

6.3.4. Minimalizacja. Firma posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

6.3.4.1. zasady zarządzania adekwatnością danych;

6.3.4.2. zasady reglamentacji i zarządzania dostępem do danych;

6.3.4.3. zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

6.3.5. Bezpieczeństwo. Firma zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

6.3.5.1. przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

6.3.5.2. przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

6.3.5.3. dostosowuje środki ochrony danych do ustalonego ryzyka;

6.3.5.4. posiada system zarządzania bezpieczeństwem informacji;

6.3.5.5. stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

7. Inwentaryzacja.

7.1. Dane niezidentyfikowane. Firma identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane, i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

7.2. Profilowanie. Firma identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych, i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Firma postępuje zgodnie z przyjętymi zasadami w tym zakresie.

7.3. Współadministrowanie. Firma identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

8. Rejestr czynności przetwarzania danych.

8.1. RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

8.2. Firma prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

8.3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Firmie rozliczanie większości obowiązków ochrony danych.

8.4. W Rejestrze dla każdej czynności przetwarzania danych, którą Firma uzna za odrębną dla potrzeb Rejestru, Firma odnotowuje co najmniej:

8.4.1. nazwę czynności przetwarzania;

8.4.2. jednostkę organizacyjną;

8.4.3. cel przetwarzania;

8.4.4. kategorię osób;

8.4.5. kategorię danych;

8.4.6. podstawę prawną;

8.4.7. źródło danych;

8.4.8. planowany termin usunięcia kategorii danych;

8.4.9. nazwę współadministratora i dane kontaktowe;

8.4.10. nazwę podmiotu przetwarzającego i dane kontaktowe;

8.4.11. kategorie odbiorców;

8.4.12. nazwę systemu lub oprogramowania;

8.4.13. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;

8.4.14. DPIA;

8.4.15. transfer do kraju trzeciego lub organizacji międzynarodowej.

8.5. Wzór Rejestru stanowi Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”. Wzór Rejestru zawiera kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Firma rejestruje informacje w miarę potrzeby i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenia się z niej.

9. Podstawy przetwarzania.

9.1. Firma dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

9.2. Wskazując w dokumentach ogólną podstawę prawną, Firma dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne.

9.3. 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 oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności.

10. Sposób obsługi praw jednostki i obowiązków informacyjnych.

10.1. Firma dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

10.2. Firma dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

10.3. Firma wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

10.4. W celu realizacji praw jednostki 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.

10.5. Firma dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

11. Obowiązki informacyjne.

11.1. Firma określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

11.2. Firma informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

11.3. Firma informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

11.4. Firma informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

11.5. Firma określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie jest to możliwe (np. tabliczka o objęciu obszaru monitoringiem).

11.6. Firma informuje osobę o planowanej zmianie celu przetwarzania danych.

11.7. Firma informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

11.9. Firma informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

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

12. Żądania osób.

12.1. Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Firma wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności, w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), Firma może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

12.2. Nieprzetwarzanie. Firma informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

12.3. Odmowa. Firma informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

12.4. Dostęp do danych. 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 realizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Firma nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

12.5. Kopie danych. Na żądanie Firma wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Firma wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.

12.6. Sprostowanie i uzupełnienie danych. Firma na żądanie osoby dokonuje sprostowania danych, uzupełnia i aktualizuje je.

12.7. Usunięcie danych. Na żądanie osoby Firma usuwa dane, gdy:

12.7.1. dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach;

12.7.2. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;

12.7.3. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;

12.7.4. dane były przetwarzane niezgodnie z prawem;

12.7.5. konieczność usunięcia wynika z obowiązku prawnego.

Firma określa sposób obsługi prawa do usunięcia danych w taki sposób, 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. W przypadku usunięcia danych Firma informuje osobę o odbiorcach danych, na żądanie tej osoby.

12.8. Ograniczenie przetwarzania. Firma dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

12.8.1. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość;

12.8.2. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

12.8.3. Firma nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

12.8.4. 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.

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.

12.9. Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Firmę na potrzeby marketingu bezpośredniego, Firma uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

13. Minimalizacja. Firma dba o minimalizację przetwarzania danych pod kątem: adekwatności danych do celów, dostępu do danych, czasu przechowywania danych.

13.1. Minimalizacja zakresu. Firma zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. Firma dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok. Firma przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

13.2. Minimalizacja dostępu. Firma stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu,

zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe). Firma stosuje kontrolę dostępu fizycznego. Firma dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób.

13.3. Minimalizacja czasu. Firma wdraża mechanizmy kontroli cyklu życia danych osobowych w Firmie, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów produkcyjnych 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 wykorzystywania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

14. Bezpieczeństwo. Firma zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Firmę.

14.1. Analiza ryzyka i adekwatności środków bezpieczeństwa. Firma przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

14.1.1. Firma zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwa i ciągłości działania;

14.1.2. Firma kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;

14.1.3. 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;

14.1.4. Firma ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Firma ustala przydatność i stosuje takie środki i podejście jak:

14.1.4.1. pseudonimizacja;

14.1.4.2. szyfrowanie danych osobowych;

14.1.4.3. inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

14.1.4.4. 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.

14.2. Oceny skutków dla ochrony danych. Firma dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie. Firma stosuje metodykę oceny skutków przyjętą w Firmie.

14.3. Środki bezpieczeństwa. Firma stosuje środki bezpieczeństwa ustalone w ramach analizy ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Firmie.

14.4. Zgłaszanie naruszeń. Firma stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

14.5. Każdy pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w Firmie zobowiązany jest do niezwłocznego poinformowania o tym ADO.

14.6. ASI, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony bazy danych zobowiązany jest do:

14.6.1. podjęcia odpowiednich działań w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej do przetwarzania danych, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych (np. fizycznego odłączenia urządzeń, wylogowania użytkownika, zmiany haseł);

14.6.2. zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem i przekazania do ADO;

14.6.3. zapisania i wydrukowania wszelkich dokumentów, które mogą pomóc w ustaleniu okoliczności, jeżeli istnieje taka możliwość;

14.6.4. przywrócenia normalnego, standardowego działania systemu (np. przez wczytanie kopii bezpieczeństwa).

14.7. Cyberbezpieczeństwo. Podłączenia urządzenia końcowego (np. komputera, terminala, drukarki, urządzenia wielofunkcyjnego) do sieci komputerowej w Firmie, może dokonać jedynie ADO lub osoba przez niego upoważniona.

14.7.1. Udostepnienie użytkownikowi zasobów sieci (np. programów), dokonywane jest przez ASI, na podstawie upoważnienia do przetwarzania danych osobowych.

14.7.2. Każde zalogowanie się użytkownika w systemie jest rejestrowane.

14.7.3. Obowiązkiem jest stosowanie co najmniej programu antywirusowego z zaporą antywłamaniową na komputerze.

14.7.4. Obowiązkiem jest dbanie o takie ustawianie ekranów monitorów, na których wyświetlane są dane osobowe, tak aby ustawienie to uniemożliwiało widok i wgląd osobom postronnym.

14.7.5. Wygaszanie ekranów monitorów i blokowanie ekranów monitorów następuje ręcznie albo automatycznie po upływie określnego czasu, nie dłuższego niż 10 min od momentu zaprzestania używania ekranu monitora.

14.7.6. Zmiana hasła do sytemu informatycznego Firmy następuje ręcznie. Zmiana hasła następuje każdorazowo w przypadku zmiany osoby upoważnionej do dostępu, do systemu informatycznego i danych.

14.8. Pomieszczenia. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe, stanowi załącznik nr 5 do niniejszego dokumentu.

14.8.1. Nadzór nad dostępem do budynków i pomieszczeń, w których przetwarzane są dane osobowe sprawuje ADO. Nadzór polega na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. Klucze do budynków lub pomieszczeń, w których przetwarzane są dane osobowe, mogą być wydane wyłącznie osobie upoważnionej do przetwarzania danych osobowych lub osobom upoważnionym do dostępu do tych budynków lub pomieszczeń.

14.8.2. Wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz. Każdy z pracowników zobowiązany jest do zamykania na klucz pomieszczeń, w których przetwarzane są dane osobowe.

14.9. Dane osobowe przechowywane w wersji papierowej lub elektronicznej (np. dyski zewnętrzne, pendrive, płyta CD albo DVD) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe w szafach metalowych lub pancernych. Klucze do szafek należy zabezpieczyć przed dostęp osób nieupoważnionych do przetwarzania danych osobowych.

15. Projektowanie prywatności. Firma zarządza zmianą mającą wpływ na prywatności w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez Firmę odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

16. Zobowiązuje się wszystkich pracowników Firmy do przestrzegania postanowień niniejszego dokumentu. Pracownicy składają pisemne oświadczenie o zapoznaniu się z niniejszą dokumentacją. Wzór oświadczenia stanowi załącznik nr 2.

17. Każda nowo przyjęta do pracy osoba zostaje zapoznana z przepisami w zakresie ochrony danych osobowych obowiązujących w Firmie, co potwierdza podpisem na oświadczeniu o poufności, którego wzór stanowi załącznik nr 2 do niniejszego dokumentu.

18. Osobę zatrudnioną oraz ubiegającą się o zatrudnienie informuje się w formie pisemnej o przetwarzaniu jej danych w związku z zatrudnieniem albo zawarciem umowy cywilnoprawnej.
19. Wszelkie prawa, w tym autorskie prawa majątkowe, do niniejszego dokumenty posiada Firma. Niniejszy dokument nie może być kopiowany ani udostępniany podmiot trzecim zarówno w celu uzyskania korzyści majątkowej jak i bez uzyskania takiej korzyści, bez uprzedniej i pisemnej zgody Firmy.

……

podpis

Załącznik nr 1

Rejestr Czynności Przetwarzania Danych Osobowych

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

Załącznik nr 2

…… ……..

imię i nazwisko miejscowość i data

Oświadczenie o poufności

Oświadczam, iż zapoznałam/em się z przepisami w zakresie ochrony danych osobowych obowiązujących w Firmie, w szczególności z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1), polityką ochrony danych osobowych obowiązującą w Firmie, a także z zasadami przetwarzania danych osobowych oraz prawami osób, których dane są przetwarzane.

Zobowiązuje się do:

1. przetwarzania danych osobowych wyłącznie w zakresie i celu niezbędnym do realizacji powierzonych przez pracodawcę/zleceniodawcę obowiązków;
2. zachowania w tajemnicy danych osobowych do których mam lub będę miała dostęp w związku z wykonywaniem obowiązków powierzonych przez pracodawcę/zleceniodawcę;
3. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych obowiązków przez pracodawcę/zleceniodawcę;
4. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;
5. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez pracodawcę/zleceniodawcę za naruszenie przepisów o ochronie danych osobowych oraz będzie traktowane jako naruszenie podstawowych obowiązków pracowniczych lub naruszenie podstawowych obowiązków zleceniobiorcy.

……

podpis

Załącznik nr 3

Informacje podawane w przypadku pozyskiwania danych osobowych od osoby, której dane dotyczą

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) informuję, że:

1. administratorem Pani/Pana danych osobowych jest firma Kursy Maturalne Potęga Wiedzy, ul. Marii Rodziewiczówny1/476, 04-187 Warszawa, reprezentowana przez Joannę Bujak - właściciela;
2. Pani/Pana dane osobowe przetwarzane będą w celu realizacji kursów, ewaluacji, oceny jakości usługi, budowania pozytywnego wizerunku Firmy na podstawie art. 6 ust. 1 lit. a), b), c) i f) RODO, czyli prawnie uzasadnionego interesu Firmy, polegającego na ułatwieniu korzystania z usług świadczonych drogą elektroniczną oraz na poprawie funkcjonalności tych usług;
3. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej;
4. Pani/Pana dane osobowe będą przechowywane przez okres minimalny wynikający z realizacji celu, w tym przez okres trwania usługi i wynikających z niej obowiązków, a następnie będą przetwarzane wyłącznie do celów finansowo-księgowych i podatkowych lub ustalenia, dochodzenia lub obrony roszczeń przez okres wymagany do momentu przedawnienia ewentualnych roszczeń;
5. posiada Pan/Pani prawo do żądania od administratora dostępu do treści swoich danych osobowych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
6. ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych narusza przepisy RODO;
7. podanie przez Panią/Pana danych osobowych jest warunkiem zawarcia umowy. Jest Pani/Pan zobowiązana/y do ich podania, a konsekwencją niepodania danych osobowych będzie korzystania z pełnej funkcjonalności systemu internetowego;
8. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania.

……
podpis

Załącznik nr 4

Informacje podawane w przypadku pozyskiwania danych osobowych

w inny sposób niż od osoby, której dane dotyczą.

Zgodnie z art. 14 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) informuję, że:

9. administratorem Pani/Pana danych osobowych jest firma Kursy Maturalne Potęga Wiedzy, ul. Marii Rodziewiczówny1/476, 04-187 Warszawa, reprezentowana przez Joannę Bujak - właściciela;
1. Pani/Pana dane osobowe przetwarzane będą w celu _____ (*należy podać cel przetwarzania*) na podstawie _____ (*należy podać podstawę prawną przetwarzania np. art. 6 ust. 1 lit. a)/b)/c)/d)/e)/f) RODO. Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – należy podać prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią*);
2. kategoria danych osobowych: dane wrażliwe/niewrażliwe;
3. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej;
4. Pani/Pana dane osobowe będą przechowywane przez okres _____ (*jeżeli nie ma możliwości wskazania okresu przechowywani należy podać kryterium ustalania tego okresu*);
5. posiada Pan/Pani prawo do żądania od administratora dostępu do treści swoich danych osobowych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (*jeżeli przetwarzanie odbywa się na podstawie zgody – art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO*), którego dokonano na podstawie zgody przed jej cofnięciem.
6. ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych narusza przepisy RODO.
7. Pani/Pana dane osobowe pozyskano z _____;
8. Pani/Pana dane będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach _____, konsekwencją takiego przetwarzania będzie _____ (*należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu*

i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą).

……

podpis

Załącznik nr 5

Rejestr budynków, pomieszczeń i części pomieszczeń, w których przetwarzane są dane osobowe

Lp.	Zbiór danych	Adres	Lokalizacja (miejsce dostępu)		Uwagi
			elektroniczna	tradycyjna papierowa	
1.					
2.					
3.					
4.					
5.					
6.					

……

podpis

Załącznik nr 6

…… ……..
pieczątka Firmy miejscowość i data

Upoważnienie nr……

dla Pani/Pana…….

Upoważniam Panią/Pana do przetwarzania danych osobowych w zbiorze/zbiorach:

……..

przy zastosowaniu …… (*nazwa systemu/systemów informatycznych przetwarzających dane osobowe*) w zakresie (WU) wglądu, (WA) wprowadzania, (MI) modyfikacji, (UA) usuwania, (AI) archiwizacji, (UM) udostępniania innym podmiotom, (KM) koniecznym do wykonywania obowiązków pracowniczych.

Równocześnie zobowiązuję Panią/Pana do zachowania tajemnicy tych danych oraz sposobów ich zabezpieczenia.

Data nadania upoważnienia: ……

Termin ważności upoważnienia:……..

……

podpis

Ja niżej podpisana/podpisany przyjęłam/przyjąłem do wiadomości zakres uprawnień wynikających z upoważnienia oraz zobowiązuje się do przestrzegania obowiązujących zasad związanych z ochroną danych osobowych. Jednocześnie oświadczam, że jestem świadoma/świadomy odpowiedzialności karnej za nieprzestrzeganie zasad związanych z ochroną danych osobowych.

……

podpis

Załącznik nr 7

Rejestr osób upoważnionych do przetwarzania danych osobowych w zbiorach

……. (nazwa zbioru)

Lp.	Imię i nazwisko	Nazwa jednostki	Data nadania upoważnienia	Termin ważności upoważnienia	Data odwołania upoważnienia	Uwagi
1.						
2.						
3.						
4.						

……

podpis

Załącznik nr 8

INFORMACJE
W SPRAWIE MONITORINGU

Na podstawie art. 22^2 Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity Dz. U. z 2018 r., poz. 917, 1000) ustalam co następuje:

1. W firmie Kursy Maturalne Potęga Wiedzy, w celu ochrony bezpieczeństwa pracowników zatrudnionych w firmie oraz zabezpieczenia mienia należącego do firmy, znajdującego się w sali szkoleniowej, a także zapobieżeniu czynom skierowanym przeciwko zatrudnionym lub mieniu Pracodawcy wprowadzam monitoring wizyjny, polegający na rejestrowaniu obrazu przez zamontowane w sali szkoleniowej kamery i inne podobne urządzenia.
2. Monitoring wizyjny będzie obejmował wejście do sali szkoleniowej, pomieszczenie dostępne dla konsumentów, zaplecze sali szkoleniowej.
3. Monitoring pomieszczeń prowadzony jest w godzinach świadczenia usług. Urządzenia są włączane i wyłączane automatycznie.
4. Jeżeli pracownicy wykonują w pomieszczeniach czynności służbowe poza normalnymi godzinami pracy, czas monitorowania ulega przedłużeniu, aż do faktycznego zakończenia czynności służbowych. Urządzenia są włączane i wyłączane automatycznie.
5. Urządzenia rejestrujące obraz znajdują się w wyłącznej dyspozycji firmy. Informacje o ich umiejscowieniu w określonych pomieszczeniach stanowią tajemnicę przedsiębiorstwa.
6. Do przeglądania zarejestrowanego obrazu oraz do kontroli urządzeń ma dostęp tylko firma.
7. Dostęp pracowników oraz osób postronnych do urządzeń rejestrujących obraz jest zabroniony, za wyjątkiem: upoważnionych pracowników serwisu urządzeń rejestrujących obraz w celu dokonania niezbędnych napraw i czynności serwisowych.
8. Obraz zarejestrowany za pomocą urządzeń monitoringu jest przechowywany na zasadach określonych w przepisach Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) – RODO i Kodeksu pracy. Podlega on zniszczeniu po upływie 3 miesięcy od zarejestrowania, chyba, że zarejestrowany obraz może być użyty lub będzie użyty jako dowód w postępowaniu prowadzonym przez właściwy sąd lub inny organ publiczny. Za przechowywanie i zniszczenie materiałów po upływie określonych prawem terminów odpowiada firma.

9. Każdy nowy pracownik przed dopuszczeniem do pracy otrzymuje pisemną informację o monitoringu na terenie sali szkoleniowej, ze wskazaniem, które pomieszczenia są objęte monitoringiem i w jakim czasie. Odpowiedzialni za przekazanie tych informacji są: firma lub upoważniona przez nią osoba.
10. Wejście do sali szkoleniowej oraz pomieszczenia sali szkoleniowej objęte monitoringiem są oznakowane tablicami z rysunkiem kamery i napisem „obiekt monitorowany”.
11. Obraz zarejestrowany za pomocą urządzeń monitoringu może zostać udostępniony uprawnionym organom publicznym, przykładowo Policji, Prokuraturze, Sądom, w zakresie prowadzonych przez organy czynności.

……

podpis

Załącznik nr 9

……..
miejscowość i data

„ZASADY CZYSTEGO BIURKA”

§ 1

„Zasady Czystego Biurka” są częścią polityki ochrony danych osobowych Kursy Maturalne Potęga Wiedzy i obowiązują wszystkich pracowników zatrudnionych w Kursy Maturalne Potęga Wiedzy, a także wszystkich zleceniobiorców, praktykantów, osoby prowadzące jednoosobową działalność gospodarczą, które współpracują z Kursy Maturalne Potęga Wiedzy.

§ 2

Przez pracownika należy rozumieć osobę zatrudnioną na podstawie umowy o pracę.

§ 3

Przez zleceniobiorców, praktykantów, osoby prowadzące jednoosobową działalność gospodarczą należy rozumieć osoby współpracujące z Kursy Maturalne Potęga Wiedzy na podstawie umowy cywilnoprawnej.

§ 4

Wskazane w § 2 i 3 osoby:

1. zobowiązane są do przechowywania na biurku tylko tych dokumentów, które są im potrzebne do wykonywania w danym momencie pracy albo wykonywania umowy cywilnoprawnej;
2. nie mogą przetrzymywać na biurku żywności lub środków spożywczych;
3. codziennie po zakończonej pracy albo zakończeniu wykonywania w danym dniu umowy cywilnoprawnej, zobowiązane są do zabezpieczenia dokumentów w zamykanej na klucz szafie;
4. zobowiązane są do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, jednakże dopiero po wcześniejszej konsultacji z Pracodawcą lub Zleceniodawcą;
5. zobowiązane są do dbania, o takie ustawienie ekranu monitora komputera, tak by ustawienie to uniemożliwiało widok i wgląd osobom postronnym.

§ 5

„Zasady Czystego Biurka” wymienione w niniejszym dokumencie obowiązują od dnia 01 stycznia 2023 r.

……

podpis