POLITYKA OCHRONY DANYCH OSOBOWYCH

w spółce Idea Complex sp. z o.o.

1. Informacje wstępne.

-

1. Niniejsza Polityka Bezpieczeństwa (dalej Polityka) ma na celu zapewnienie zgodności działania spółki Idea Complex sp. z o.o. z siedzibą w Łodzi (dalej Spółka) jako Administratora Danych Osobowych z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych. Polityka opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Ma ona stanowić zbiór wymogów, zasad i regulacji ochrony danych osobowych w Spółce.
2. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Zarząd Spółki.
3. Odpowiedzialny za nadzór i monitorowanie przestrzegania Polityki jest Zarząd lub Inspektor Ochrony Danych w przypadku jego powołania.
4. Dokument Polityki Bezpieczeństwa został opracowany w oparciu o:
    0. ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (U. 2018 r. poz. 1000) ;
    1. 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 [rozporządzenie ogólne o ochronie danych];
5. Obszarem przetwarzania danych osobowych przez Spółkę jest każdorazowy adres siedziby spółki oraz każdorazowy adres siedziby podmiotów, które przetwarzają dane osobowe na zlecenie administratora.

1. Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
2. 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).
3. Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
4. Dane wrażliwe oznaczają dane specjalne i dane karne.
5. Dane specjalne oznaczają 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.
6. Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
7. Dane dzieci oznaczają dane osób poniżej 16. roku życia.
8. Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
9. Podmiot przetwarzający oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).
10. 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.

11. Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
12. IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych
13. RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
14. Spółka oznacza spółkę Idea Complex sp. z o.o. z siedzibą w Łodzi (90-212), przy ul. Sterlinga 27/29, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod nr KRS: 0000782442, prowadzonego przez Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, NIP: 7252288665.

- <u>Ochrona danych osobowych w Spółce – zasady ogólne</u>
    0. Filary ochrony danych osobowych w Spółce:

1. Legalność - Spółka dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
2. Bezpieczeństwo - Spółka zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
3. Prawa Jednostki - Spółka umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
4. Rozliczalność - Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.
    2. Zasady ochrony danych

Spółka przetwarza dane osobowe z poszanowaniem następujących zasad:

1. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2. rzetelnie i uczciwie (rzetelność);
3. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
4. w konkretnych celach i nie ‚na zapas" (minimalizacja);
5. nie więcej niż potrzeba (adekwatność);
6. z dbałością o prawidłowość danych (prawidłowość);
7. nie dłużej niż potrzeba (czasowość);
8. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

3. System ochrony danych

System ochrony danych osobowych w Spółce składa się z następujących elementów:

- Inwentaryzacja danych. Spółka dokonuje identyfikacji zasobów danych osobowych w Spółce, w tym:

1. przypadków przetwarzania danych specjalnych i danych „kryminalnych" (dane wrażliwe);
2. przypadków przetwarzania danych osób, których Spółka nie identyfikuje (dane niezidentyfikowane);
3. przypadków przetwarzania danych dzieci;
4. profilowania;
5. współadministrowania danymi.

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

1. utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
2. inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Spółka przetwarza dane na podstawie prawnie uzasadnionego interesu Spółki.

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

1. Obowiązki informacyjne. Spółka przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
2. Możliwość wykonania żądań. Spółka weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

3. Obsługa żądań. Spółka zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
4. Zawiadamianie o naruszeniach. Spółka stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

- Spółka posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

1. zasady zarządzania adekwatnością danych;
2. zasady reglamentacji i zarządzania dostępem do danych;
3. zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności;

- Bezpieczeństwo. Spółka zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

1. przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
2. przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
3. dostosowuje środki ochrony danych do ustalonego ryzyka;
4. posiada system zarządzania bezpieczeństwem informacji;
5. stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych - zarządza incydentami.

- Przetwarzający. Spółka posiada zasady doboru przetwarzających dane na rzecz Spółki, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
- Eksport danych. Spółka posiada zasady weryfikacji, czy Spółka nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

- *Privacy by design*. Spółka zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Spółce uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.
- Przetwarzanie transgraniczne. Spółka posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

1.
    0. Dane specjalne

Spółka identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe (dane specjalne i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Spółka postępuje zgodnie z przyjętymi zasadami w tym zakresie.

1. Dane niezidentyfikowane

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

1. Profilowanie

Spółka 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, Spółka postępuje zgodnie z przyjętymi zasadami w tym zakresie.

1. Współadministrowanie

Spółka identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

1. Podstawy przetwarzania.
    0. Spółka wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
    1. Kierownik komórki organizacyjnej Spółki ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Spółki, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Spółki.
2. Sposób obsługi praw jednostki i obowiązków informacyjnych
    0. Spółka dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
    1. Spółka ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Spółki informacji lub odwołania (linki) do informacji o prawach osób, sposobie skorzystania z nich w Spółce, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Spółką w tym celu, ewentualnym cenniku żądań ‚dodatkowych" itp.
    2. Spółka dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
    3. Spółka wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
    4. W celu realizacji praw jednostki Spółka zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Spółkę, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

5. Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

- Obowiązki informacyjne
    0. Spółka określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
    1. Spółka informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
    2. Spółka informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
    3. Spółka informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
    4. Spółka określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
    5. Spółka informuje osobę o planowanej zmianie celu przetwarzania danych.
    6. Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania.
    7. Spółka informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
    8. Spółka informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
    9. Spółka bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
- Żądania osób
    0. Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Spółka 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 itp.), Spółka może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

1. Nieprzetwarzanie. Spółka informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
2. Odmowa. Spółka informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
3. Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych, Spółka informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Spółka nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
4. Kopie danych. Na żądanie Spółka wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Spółka wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.
5. Sprostowanie danych. Spółka dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Spółka ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

6. Uzupełnienie danych. Spółka uzupełnia i aktualizuje dane na żądanie osoby. Spółka ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Spółka nie musi przetwarzać danych, które są Spółce zbędne). Spółka może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Spółkę procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
7. Usunięcie danych. Na żądanie osoby, Spółka 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.

Spółka 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.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Spółkę, Spółka podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

1. Ograniczenie przetwarzania. Spółka 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 danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
3. Spółka nie potrzebuje już danych osobowych, 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.

W trakcie ograniczenia przetwarzania Spółka przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

1. Przenoszenie danych. Na żądanie osoby Spółka wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Spółce, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Spółki.
2. Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes

Spółki lub o powierzone Spółce zadanie w interesie publicznym, Spółka uwzględni sprzeciw, o ile nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

3. Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli Spółka prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Spółka uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
4. Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Spółkę na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Spółka uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
5. Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli Spółka przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Spółka zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Spółki, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Spółką; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

1. Minimalizacja.

1. Spółka dba o minimalizację przetwarzania danych pod kątem: (i) adekwatności danych do celów (ilości danych i zakresu

przetwarzania), (ii) dostępu do danych, (iii) czasu przechowywania danych.

2. Spółka zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
3. Spółka dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
4. Spółka przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).
5. Spółka 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).
6. Spółka stosuje kontrolę dostępu fizycznego.
7. Spółka dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
8. Spółka dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
9. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Spółki.
10. Spółka wdraża mechanizmy kontroli cyklu życia danych osobowych w Spółce, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.
11. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów produkcyjnych Spółki, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Spółkę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

1. Bezpieczeństwo.

1. Spółka zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Spółkę.
2. Spółka przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

1. Spółka zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania - wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
2. Spółka kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
3. Spółka przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Spółka analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
4. Spółka ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Spółka ustala przydatność i stosuje takie środki i podejście jak:
5. szyfrowanie danych osobowych,
6. inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

- 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.

1. Spółka dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

2. Spółka stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
3. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Spółce i są bliżej opisane w procedurach przyjętych przez Spółkę dla tych obszarów.
4. Spółka stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.
5. Przetwarzający
6. Spółka posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Spółki opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Spółce.
7. Spółka przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące, załącznik do niniejszej Polityki.
8. Spółka rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z zasad powierzenia danych osobowych.

- Eksport Danych.

Spółka rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Spółka okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

- Projektowanie Prywatności.

Spółka zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

W tym celu zasady prowadzenia projektów i inwestycji przez Spółkę odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

- Monitoring wizyjny.

1. W celu zapewnienia bezpieczeństwa osób i mienia, wprowadza się monitoring wizyjny na części obszaru siedziby Spółki.
2. Obszar monitorowany oznaczany jest specjalnymi tablicami informacyjnymi.
3. Nagrania z monitoringu przechowywane są tak długo, jak technicznie dostępne jest miejsce na dysku urządzenia rejestrującego, nie dłużej jednak niż 3 miesiące.
4. Monitoring może być wykorzystywany wyłącznie w celu zapewnienia bezpieczeństwa osób i mienia. W szczególności, nie może być wykorzystywany do prowadzenia kontroli czasu i jakości pracy pracowników.
5. Informacja o każdym incydencie bezpieczeństwa, do rozwiązania którego konieczne było skorzystanie z monitoringu, odnotowywana jest w dokumentacji incydentów z określeniem czasu incydentu, krótkim opisem samego incydentu oraz wymienieniem osób, które przeglądały nagrania lub którym nagrania udostępniono.
6. W przypadku rozwiazywania incydentu bezpieczeństwa osób lub mienia nie wymagającego udziału służb zewnętrznych (Straży Miejskiej, Policji, itp.)
    0. nagrania przeglądane są bez ich przegrywania na nośniki zewnętrzne,

    1. osoby trzecie zapoznawane są wyłącznie z tymi fragmentami nagraniá, które bezpośrednio dotyczą incydentu,
    2. nagrania nie są udostępniane osobom trzecim w inny sposób, niż poprzez ich pokazanie pod kontrolą osób uprawnionych.
7. W przypadku incydentu wymagającego udziału służb zewnętrznych (Straży Miejskiej, Policji, itp.), dopuszcza się przekazanie wybranych fragmentów nagrań tym służbom, jedynie w przypadku rozwiązywania incydentu bezpieczeństwa osób lub mienia
    0. po odebraniu pisemnego i uzasadnionego wniosku
    1. oraz po odebraniu pisemnego protokołu przekazania zawierającego informacje o tym, jaki zakres czasowy i obszarowy nagrań został przekazany oraz kto (imię, nazwisko, stopień) odebrał nagranie w imieniu służb.
8. Zabrania się przekazywania komukolwiek, poza uprawnionymi służbami, nagrań.
9. Dopuszcza się, na uzasadniony wniosek osoby trzeciej, zarchiwizowanie części nagrań, które mogą być podstawą do dochodzenia przez tę osobę roszczeń zarówno wobec innej osoby trzeciej, jak i samego ADO. Tak zarchiwizowane nagrania mogą być przekazane tylko odpowiednim służbom, chyba że zawierają wyłącznie treści, których udostepnienie nie naruszy praw i wolności innych osób.
10. Rejestrator cyfrowy znajduje się w zamykanym pomieszczeniu, w oddzielnie zamykanej szafce.
11. Dostęp do nagrań wymaga podania oddzielnego loginu i hasła.
12. Monitor wyświetlający podgląd na żywo, ustawiony jest w sposób uniemożliwiający wgląd w nagrania osobom trzecim.
13. Podczas przeglądania nagrań, monitor ustawiany jest w taki sposób, aby nagrania były przeglądane wyłącznie przez osoby uprawnione do wglądu.

1. <u>Polityka Czystego Biurka.</u>

1. Niniejsza polityka czystego biurka obowiązuje wszystkich pracowników zatrudnionych w Spółce.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, praktykanta i stażystę, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z.
3. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.
4. Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu.
5. Po zakończonej pracy pracownik zobowiązany jest zabezpieczyć wszystkie dokumenty w sposób, który uniemożliwi do nich dostęp osobom niepowołanym.
6. Po zakończonej pracy pracownik zobowiązany jest wyłączyć komputer.
7. Po zakończonej pracy na biurku mogą znajdować się jedynie telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis, itp.
8. Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.

- Postanowienia końcowe.

1. Niniejsza dokument wszedł w życie z datą podjęcia uchwały przez Zarząd.
2. Wszelki zmiany niniejszej Polityki wymagają zachowania formy pisemnej pod rygorem nieważności i podjęcia w tym przedmiocie uchwały Zarządu.

Wykonując obowiązek wynikający z art. 14 ust. 1 i ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (RODO) prosimy o potwierdzenie akceptacji poniższych oświadczeń własnym imieniem i nazwiskiem. Odpowiedź na wiadomość oznacza udzielenie zgody. Wyrażenie zgody jest dobrowolne.

Oświadczam, że dane podane w niniejszym formularzu podaję dobrowolnie, potwierdzam ich prawdziwość oraz wnoszę na ich podstawie o przygotowanie oferty sprzedaży instalacji fotowoltaicznej. Oświadczam tym samym, że zapoznałam/em się z treścią Informacji o Administratorze danych osobowych i zasadach ich przetwarzania umieszczony pod adresem: www.nieplacezaprad.pl/rodo. Potwierdzam także otrzymanie informacji, że Administratorem moich danych osobowych jest Idea Complex sp. z o.o. z siedzibą w Łodzi przy ul. Dra Seweryna Sterlinga 27/29 (kod: 90-212 Łódź). Zostałam/zostałem poinformowany o prawie do sprostowania podanych danych, możliwości ograniczenia ich przetwarzania oraz prawie do ich całkowitego usunięcia w każdym momencie bez konieczności podawania przyczyny.

Wyrażam zgodę na prowadzenie przez Idea Complex sp. z o.o. działań marketingowych w formie rozmowy telefonicznej oraz SMS/MMS oraz na przesyłanie na podany przeze mnie adres e-mail informacji handlowych. Zostałam/em poinformowana/y, że wszelkie pytania dotyczące przetwarzanych danych osobowych mogę kierować za pośrednictwem korespondencji na adres: rodo@nieplacezaprad.pl.