

Polityka ochrony danych osobowych w u administratora danych osobowych, Mateusza Józwiaka prowadzącego działalność gospodarczą pod nazwą „MATSTAL” Mateusz Józwiak, Kamień Kolonia 12a, 62 – 834 Ceków, NIP: 9680939240, REGON: 301644032

Z uwagi na:

- 1) konieczność dostosowania ochrony i przetwarzania danych osobowych u administratora, Mateusza Józwiaka, prowadzącego działalność gospodarczą pod nazwą „MATSTAL” Mateusz Józwiak, Kamień Kolonia 12a, 62 – 834 Ceków, NIP: 9680939240, REGON: 301644032 (zwanego dalej „Administratorem”) do przepisów 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) (dalej „**RODO**”),
- 2) zwiększenie ochrony i bezpieczeństwa danych osobowych przetwarzanych u Administratora
- 3) zwiększenie świadomości pracowników Administratora w zakresie ochrony danych osobowych,
- 4) zwiększenie ochrony praw i wolności osób fizycznych, których dane osobowe są przetwarzane u Administratora

- niniejszym wprowadza się Politykę ochrony danych osobowych u Administratora.

Postanowienia wstępne

§ 1

Polityka zawiera:

- 1) opis zasad i systemów ochrony danych osobowych obowiązujących u Administratora,
- 2) opis systemu obsługi praw jednostki i obowiązków informacyjnych obowiązujący u Administratora,
- 3) ogólny opis stosowanych reguł bezpieczeństwa odnośnie danych osobowych u Administratora.

§ 2

Odpowiedzialność za wdrożenie i utrzymanie Polityki ponosi Administrator, który sprawuje stały nadzór nad przestrzeganiem wszelkich postanowień Polityki przez pracowników Administratora.

§ 3

Za stosowanie postanowień Polityki odpowiedzialni są:

- 1) Administrator,
- 2) pracownicy Administratora.

Słownik pojęć

§ 4

Pojęcia zawarte w Polityce oznaczają:

- 1) **Polityka** – oznacza niniejszą Politykę ochrony danych osobowych u Administratora, o ile co innego nie wynika wyraźnie z kontekstu,
- 2) **Administrator** – oznacza Mateusza Józwiaka prowadzącego działalność gospodarczą pod nazwą „MATSTAL” Mateusz Józwiak, Kamień Kolonia 12a, 62 – 834 Ceków, NIP: 9680939240, REGON: 301644032,
- 3) **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),
- 4) **Dane** – oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu,
- 5) **Dane szczególnych kategorii** – 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 dzieci** – oznaczają dane osób poniżej 16 roku życia,
- 7) **Osoba** – oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu,
- 8) **Podmiot przetwarzający** – oznacza organizację lub osobę, której Administrator powierzył przetwarzanie danych osobowych
- 9) **Eksport danych** – oznacza przekazanie danych do Państwa Trzeciego (rozumianego jako Państwo spoza Europejskiego Obszaru Gospodarczego) lub do organizacji międzynarodowej,
- 10) **RCPD** – oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

Zasady ochrony danych

§ 5

1. Do podstawowych zasad ochrony danych u Administratora należą:
 - 1) **legalność** – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem,
 - 2) **bezpieczeństwo** – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stałe działania w tym zakresie oraz dokonując regularnej analizy ryzyka,
 - 3) **ochrona praw jednostki** – Administrator umożliwia osobom, których dane przetwarza wykonywanie wszystkich swoich praw,
 - 4) **rozliczalność** – Administrator dokumentuje, w jaki sposób spełnia obowiązki przewidziane niniejszą Polityką oraz treścią RODO, aby w każdej chwili móc wykazać zgodność przetwarzania danych u Administratora z Polityką i RODO.
2. Administrator przetwarza dane osobowe przy uwzględnieniu następujących zasad:

- 1) w oparciu o podstawę prawną i zgodnie z prawem (**legalność**),
- 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 jest potrzebne (**adekwatność**),
- 6) z dbałością o prawidłowość danych (**prawidłowość**),
- 7) nie dłużej niż potrzeba (**czasowość**),
- 8) zapewniając odpowiednie bezpieczeństwo danych (**bezpieczeństwo**).

Elementy systemu ochrony danych

§ 6

System ochrony danych u Administratora składa się z następujących elementów:

- 1) **inwentaryzacja danych** – Administrator dokonuje identyfikacji zasobów przetwarzanych danych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w tym:
 - a) przypadków przetwarzania danych szczególnych kategorii, w szczególności danych dotyczących zdrowia,
 - b) przypadków przetwarzania danych osób, których Administrator nie identyfikuje (dane niezidentyfikowane),
 - c) przypadków przetwarzania danych dzieci,
 - d) ewentualnego współadministrowania danymi,
- 2) **RCPD** – Administrator opracowuje, prowadzi i utrzymuje RCPD. RCPD jest narzędziem rozliczania zgodność z ochroną danych u Administratora,
- 3) **podstawy prawne** – Administrator zapewnia i weryfikuje podstawy prawne przetwarzania danych u Administratora oraz wskazuje je w RCPD,
- 4) **obsługa praw jednostki** – Administrator zapewnia obsługę praw osób fizycznych, których dane są przetwarzane u Administratora oraz spełnia obowiązki informacyjne względem tych osób, a w szczególności Administrator spełnia i zapewnia:
 - a) obowiązki informacyjne – Administrator udostępnia osobom wymagane informacje przy zbieraniu danych tych osób,
 - b) możliwość wykonywania żądań – Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego przewidzianego prawem typu żądania przez siebie i swoich przetwarzających,
 - c) obsługa żądań – Administrator zapewnia odpowiednie procedury, aby żądania osób były dokumentowane i realizowane w terminach oraz w sposób wymagany przez RODO,
 - d) zawiadomienie o naruszeniach – Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych,
- 5) **minimalizacja** – Administrator posiada zasady i metody zarządzania minimalizacją danych (*privacy by default*), w tym zasady zarządzania adekwatnością danych, zasady reglamentacji dostępem do danych (gradacja danych), zasady zarządzania okresem przechowywania danych i weryfikacji ich dalszej przydatności,

- 6) **bezpieczeństwo** – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
 - a) przeprowadza okresowe analizy ryzyka dla czynności przetwarzania danych,
 - b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,
 - c) stosuje środki ochrony w celu zmniejszenia wysokości ryzyka,
 - d) stosuje procedury pozwalające na identyfikację incydentu naruszenia bezpieczeństwa danych i zgłoszenia naruszenia organowi nadzorczemu,
- 7) **przetwarzający** – Administrator zawiera umowy o powierzenie przetwarzania danych z podmiotami, które te dane przetwarzają oraz weryfikuje wykonywanie umów powierzania przez te podmioty,
- 8) **upoważnienia** – Administrator udziela pracownikom stosownych upoważnień do przetwarzania danych osobowych oraz prowadzi rejestr udzielonych i odwołanych upoważnień,
- 9) **eksport danych** – Administrator sprawuje nadzór nad tym, czy dane przetwarzane przez Administratora są przekazywane do Państwa Trzeciego lub organizacji międzynarodowej,
- 10) **privacy by design** – wszelkie projekty i inwestycje u Administratora i realizowane przez Administratora uwzględniają od samego początku konieczność oceny ryzyka związanego z ochroną danych i zapewnieniem prywatności.

§ 7

1. Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne oraz opiera je na podstawach prawnych przewidzianych przez RODO.
2. Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
3. Administrator identyfikuje przypadki, w których dokonuje profilowania przetwarzania danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Administrator postępuje zgodnie z ustalonymi w RODO zasadami.
4. Administrator weryfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z ustalonymi w RODO zasadami, a w szczególności zawiera umowy o współadministrowanie danymi.

RCPD

§ 8

1. Administrator prowadzi RCPD, który jest formą 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, czyli zasady rozliczalności.

2. W RCPD Administrator inwentaryzuje i monitoruje sposób, w jaki przetwarza się dane osobowe.
3. W RCPD Administrator odnotowuje co najmniej:
 - 1) nazwę czynności przetwarzania,
 - 2) cel przetwarzania,
 - 3) opis kategorii osób,
 - 4) opis kategorii danych,
 - 5) podstawę prawną przetwarzania wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora, jeśli podstawą prawną przetwarzania danych jest uzasadniony interes Administratora,
 - 6) źródło danych,
 - 7) planowany termin usunięcia danych (jeżeli jego precyzyjne określenie jest możliwe),
 - 8) nazwę współadministratora (jeśli dotyczy),
 - 9) nazwę podmiotu przetwarzającego (jeśli dotyczy),
 - 10) opis kategorii odbiorców,
 - 11) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,
 - 12) informację o przekazaniu danych poza Europejski Obszar Gospodarczy.

§ 9

1. Administrator dokumentuje w RCPD podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
2. Administrator stosuje metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej danych osobowych w określonym celu, a także rejestrację odmowy i cofnięcia zgody.

Informowanie

§ 10

1. Administrator kładzie szczególny nacisk na czytelność, klarowność i rzetelność przekazywanych informacji osobom, których dane przetwarza.
2. Administrator podejmuje działania w celu ułatwienia osobom, których dane przetwarza realizację ich praw w tym poprzez:
 - a) zamieszczenie na stronie internetowej Administrator informacji o prawach osób, których dane są przetwarzane,
 - b) zamieszczania w stopce maili kierowanych Administrator i jego pracowników do innych osób podstawowych informacji o Administratorze oraz linków do informacji zamieszczonych na stronie internetowej Administratora,,
 - c) zamieszczanie w miejscach widocznych w biurach Administratora oraz pomieszczeniach, w których wykonywana jest praca informacji w formie papierowej o prawach osób, których dane dotyczą.
3. Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób, których dane przetwarza.

4. Administrator stosuje adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw tych osób i obowiązków informacyjnych.
5. Administrator dokumentuje obsługę zawiadomień i żądań osób.

§ 11

1. Administrator stosuje zgodnie z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
2. Administrator informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
3. Administrator informuje osobę o przetwarzaniu jej danych przy pozyskiwaniu danych od tej osoby.
4. Administrator informuje osobę o przetwarzaniu jej danych przy pozyskiwaniu danych z innego źródła aniżeli ta osoba.
5. Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych tam, gdzie jest to możliwe.
6. Administrator informuje osobę o planowanej zmianie celu przetwarzania danych.
7. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.
8. Administrator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe.
9. Administrator bez zbędnej zwłoki informuje osobę o naruszeniu ochrony danych osobowych, jeżeli może ono spowodować wysokie ryzyko naruszenia praw i wolności tej osoby.

Obsługa żądań osób

§ 12

1. Przy realizacji i ochronie praw osób, których dane dotyczą, Administrator wprowadza procedury gwarantujące ochronę praw i wolności osób trzecich.
2. W przypadku powzięcia wiarygodnej informacji 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. związane z ochroną danych innych osób, ochroną prawa własności intelektualnej, tajemnicą handlową, tajemnicą przedsiębiorstwa, ochroną dóbr osobistych), Administrator może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu tej osoby.
3. Jeśli Administrator nie przetwarza danych osoby składającej żądanie dotyczące jej praw, Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących.
4. Administrator w terminie miesiąca informuje osobę o odmowie rozpatrzenia jej żądania i o prawach tej osoby z tym związanych.
5. Na żądanie osoby dotyczące dostępu do jej danych Administrator informuje osobę o tym, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania –

stosownie do art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących.

6. Na żądanie osoby Administrator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator ustala cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.
7. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych na żądanie osoby, Administrator informuje tę osobę o odbiorcach danych.
8. Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

§ 13

1. Na żądanie osoby Administrator usuwa dane, gdy:
 - 1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych zgodnych z prawem celach,
 - 2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy przetwarzania,
 - 3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
 - 4) dane były przetwarzane niezgodnie z prawem,
 - 5) konieczność usunięcia wynika z obowiązku prawnego.
2. Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym zasad bezpieczeństwa, a także weryfikację czy w danym wypadku nie zachodzą wyjątki, o których mowa w art. 17 ust. 3 RODO.
3. Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich.
4. W przypadku usunięcia danych, Administrator – na żądanie osoby, której dane zostały usunięte – informuje tę osobę o odbiorcach danych.

§ 14

1. Administrator 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, żądając w zamian ograniczenia ich przetwarzania,
 - 3) Administrator nie potrzebuje już danych, 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 Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
2. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń albo w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
3. Administrator, przed uchynieniem ograniczenia przetwarzania, informuje o tym osobę, której dane dotyczą.
4. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

§ 15

Na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi – jeżeli jest to możliwe – dane dotyczące tej osoby, które ta osoba dostarczyła Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej.

§ 16

Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes Administratora lub w oparciu o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

Minimalizacja przetwarzania danych

§ 17

1. Administrator dba o minimalizację przetwarzania danych pod kątem:
 - 1) adekwatności danych do celów,
 - 2) dostępu do danych,
 - 3) czasu przechowywania danych.
2. Administrator weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania.
3. Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

4. Administrator stosuje ograniczenia dostępu do danych:
 - 1) prawne (w szczególności: zobowiązania do poufności, zakresy upoważnień),
 - 2) fizyczne (strefy dostępu, zamykanie pomieszczeń),
 - 3) logiczne (ograniczenie uprawnień do systemów przetwarzających dane zasobów sieciowych).
5. Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.
6. Administrator wdraża mechanizmy kontroli cyklu życia danych u Administratora, w tym weryfikacji dalszej przydatności danych względem terminów wskazanych w RCPD.
7. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów Administratora, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Administratora. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystywania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym również wymogi usuwania danych.

Bezpieczeństwo danych

§ 18

1. Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych przez Administratora.
2. Administrator regularnie przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych. W tym celu:
 - 1) Administrator zapewnia, że jego pracownicy posiadają odpowiedni stan wiedzy o bezpieczeństwie danych i ciągłości przetwarzania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych,
 - 2) Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają,
 - 3) Administrator przeprowadza analizy ryzyka naruszenia praw i wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator okresowo analizuje możliwe sytuacje i scenariusze naruszenia danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia,
 - 4) Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. Administrator, stosuje środki ochrony danych, które zostały szczegółowo określone w Regulaminie bezpieczeństwa danych stanowiącej odrębny dokument. Regulamin bezpieczeństwa ma charakter niejawnny i dostęp do jej treści posiadają tylko osoby upoważnione.
3. Administrator stosuje środki bezpieczeństwa ustalone w ramach dokonanych analiz i audytów.
4. Wszyscy pracownicy Administratora zobowiązują się do przestrzegania reguł bezpieczeństwa opisanych w niniejszej Polityce oraz Regulaminie bezpieczeństwa, a

także do stosowania wszelkich wymaganych prawem oraz zasadami doświadczenia życiowego środków ostrożności w celu ochrony danych.

5. W przypadku zaniechania stosowania przez pracowników reguł bezpieczeństwa opisanych w niniejszej Polityce, Administrator ma prawo stosować przewidziane prawem środki dyscyplinujące lub inne środki w celu ochrony dobra Administratora oraz jej roszczeń.

§ 19

1. Administrator podejmuje wszelkie możliwe działania w celu przeciwdziałania incydentom naruszenia ochrony danych, a w przypadku ich wystąpienia – w celu zminimalizowania skutków tych incydentów.
2. Szczegółowa wewnętrzna procedura w przypadku wystąpienia incydentu naruszenia danych osobowych została określona w Regulaminie bezpieczeństwa obowiązującym u Administratora.

Podmioty przetwarzające

§ 20

1. Administrator stosuje zasady ostrożności oraz reguły doboru i weryfikacji przetwarzających dane na rzecz Administratora 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 Administratorze.
2. Administrator zawiera z podmiotami przetwarzającymi umowy o powierzenie przetwarzania danych osobowych.
3. Administrator rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z przyjętych reguł powierzenia danych.

Eksport danych

§ 21

Administrator rejestruje w RCPD przypadki eksportu danych.

Wiedza i szkolenia

§ 22

1. Administrator dokłada wszelkich starań, aby wszyscy jego pracownicy posiadali jak najlepszą i jak najbardziej aktualną wiedzę z zakresu ochrony danych.
2. W celu określonym w powyższym ustępie, Administrator przeprowadza szkolenia z zakresu przetwarzania i ochrony danych, w których obowiązek uczestniczenia mają wszyscy pracownicy Administratora.

Postanowienia końcowe

§ 23

1. Administrator zapozna z treścią niniejszego Regulaminu wszystkich swoich pracowników. Zapoznanie nastąpi w oparciu o oświadczenie, którego wzór stanowi załącznik nr 1 do niniejszej Polityki
2. Polityka wchodzi w życie z momentem zapoznania się z jej treścią wszystkich aktualnych pracowników Administratora tj. z momentem podpisania przez nich oświadczenia, którego wzór stanowi załącznik nr 1 do niniejszej Polityki.


"MATSTAL"
Mateusz Józwiak
62-834 Ceków, Kamień Kolonia 12A
tel: 662 198 166
NIP 968-093-92-40 REGON 301644032