PGZ ZMM

CCJ
AQAP 2110:2016
PN-EN ISO 9001:2015
WSK

Polityka Bezpieczeństwa Ochrony Danych Osobowych w Spółce Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A. w Zabrzu

Z DNIA 15.01.2021 r.

Pieczęć:	ZAKŁAD MECHANICZNY "BUMAR-MIKULCZYCE" Spółka Akcyjna 41-807 Zabrze, ul. Handlowa 2 tel. +48 32 373-86-00 do 699 fax +48 32 271-37-42 Regon 271830823 NIP 648-10-00-642	
Zatwierdził:		**Data:**
PREZES ZARZĄDU DYREKTOR NACZELNY Tomasz Polus		15.01.2021 r.

Spis treści.

Polityka Bezpieczeństwa Ochrony Danych Osobowych

I. Wstęp

1. Informacje ogólne

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Zakładzie Mechanicznym „BUMAR-MIKULCZYCE" S.A. grupy informacji zawierającej dane osobowe.

Opisane i zastosowane w niej zabezpieczenia mają zapewnić:

1) **poufność danych** - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2) **integralność danych** - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3) **rozliczalność danych** - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4) **integralność systemu** - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

2. Cel przygotowania Polityki Bezpieczeństwa

Podstawowym celem przygotowania i wdrożenia dokumentu jest zapewnienie zgodności działania Zakładu z Rozporządzeniem 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) oraz Polskim regulacjom prawnym.

Zakres przedmiotowy stosowania niniejszej Polityki obejmuje wszystkie zbiory danych osobowych przetwarzane zarówno w formie elektronicznej jaki w formie papierowej.

Polityka obowiązuje wszystkich pracowników Zakładu Mechanicznego „BUMAR-MIKULCZYCE" S.A. oraz podmioty współpracujące przy przetwarzaniu danych oraz osoby przebywające na obszarze przetwarzania danych osobowych.

3. Zakres informacji objętych polityką bezpieczeństwa oraz zakres stosowania

Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zbiór działań zmierzających do uzyskania i utrzymania wymaganego poziomu bezpieczeństwa danych osobowych, tj.

zapewnienie poufności, spójności i dostępności na każdym etapie tworzenia, przetwarzania, przechowywania i przesyłania danych osobowych.

Polityka Bezpieczeństwa, odnosi się całościowo do problemu zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie, jak i w systemach informatycznych w odniesieniu, do których w przypadku szczegółowych regulacji występuje odesłanie do Instrukcji Zarządzania Systemem Informatycznym.

Jako załącznik do niniejszej polityki opracowano i wdrożono procedury w postaci Instrukcji Zarządzania Systemem Informatycznym. Określają one sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, oraz danych osobowych poza systemem informatycznym ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

II. Definicje

1. **Polityka** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych.
2. **Administrator Danych Osobowych (ADO) –** Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A. z siedzibą w Zabrzu (41–800) przy ul. Handlowej 2 NIP: 6481000642.
3. **RODO** – rozumie się przez to 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. **Organ nadzorczy -** niezależny organ publiczny ustanowiony przez państwo polskie (Prezes Urzędu Ochrony Danych Osobowych).
5. **Administrator Systemów Informatycznych (ASI) –** Osoba odpowiedzialna za systemy informatyczne funkcjonujące w Zakładzie.
6. **Inspektor Ochrony Danych [IOD]** - powołana pisemnie przez ADO osoba, która w imieniu ADO sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych oraz wypełnia inne zadania opisane a art. 39 RODO.
7. **Dane osobowe (dane)** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
8. **Szczególna kategoria danych -** Są to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby oraz dane genetyczne i dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej.

9. **Pseudominizacja -** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
10. **Anonimizacja -** uniemożliwia wszystkim stronom wyodrębnienie konkretnej osoby fizycznej ze zbioru danych. Uniemożliwia też, tworzenie powiązań między dwoma zapisami w zbiorze danych (lub między dwoma oddzielnymi zbiorami) i wnioskowanie jakichkolwiek informacji z tych danych.
11. **Zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, dostępnych wg. określonych kryteriów.
12. **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
13. **Baza danych osobowych** - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych na nośniku informatycznym lub papierowym. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe.
14. **Przetwarzanie danych** - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie.
15. **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
16. **Administrator systemu (Informatyk)** - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.
17. **Użytkownik** – osoba posiadająca uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych lub zleceniem.
18. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów informacyjnych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
19. **Nośnik danych** – nośnik służący do zapisu i przechowywania informacji w wersji elektronicznej lub papierowej.
20. **Praca zdalna** – wykonywanie zadań powierzonych przez pracodawcę poza siedzibą firmy.

III. Odpowiedzialność w zakresie zarządzania bezpieczeństwem.

1. Deklaracja

Administrator Danych mając świadomość, że przetwarza dane osobowe, w tym dane osobowe pracowników deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa. Administrator danych deklaruje stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A. w zakresie przetwarzania danych osobowych dąży, aby dane osobowe były:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu");
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

Przez bezpieczeństwo danych osobowych rozumie się zabezpieczenie tych danych, poprzez wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich przetwarzaniem niezgodnym z przepisami prawa.

Zakres przedmiotowy stosowania niniejszej Polityki obejmuje wszystkie zbiory danych osobowych przetwarzane zarówno w formie elektronicznej jaki w formie papierowej.

Polityka obowiązuje wszystkich pracowników Zakładu Mechanicznego „BUMAR-MIKULCZYCE" S.A. oraz podmioty współpracujące przy przetwarzaniu danych oraz osoby przebywające na obszarze przetwarzania danych osobowych.

2. Administrator danych - zadania i obowiązki

1) ADO obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
2) realizuje obowiązek informacyjny wobec osoby, której dane dotyczą oraz przestrzega praw osoby, której dane dotyczą, m.in. prawa do dostępu oraz zapomnienia;
3) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
4) powołuje Inspektora Ochrony Danych;
5) wyznacza Administratora Systemu Informatycznego;
6) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych;
7) zapewnia przetwarzanie danych zgodnie z uregulowaniami Polityki Bezpieczeństwa Informacji, sprawuje nadzór nad bezpieczeństwem danych osobowych.

3. IOD – zadania i obowiązki

1) informowanie administratora, podmiotów przetwarzających oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych wymagań prawnych;
2) monitorowanie przestrzegania RODO, innych wymagań prawnych dotyczących ochrony danych osobowych oraz Polityki Bezpieczeństwa Ochrony Danych w tym podział obowiązków, działania zwiększające świadomość, szkolenia określonych pracowników uczestniczących w operacjach przetwarzania oraz powiązane z tym audity;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z konsultacjami związanymi oceną skutków dla ochrony danych oraz we wszelakich innych sprawach;

6) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO;
7) prowadzenie rejestru czynności przetwarzania.

4. Osoba upoważniona do przetwarzania danych

1) Może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy bądź odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.
2) Musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora Danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.
3) Musi zapoznać się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki Bezpieczeństwa.
4) Stosuje określone przez Administratora Danych oraz Inspektora Ochrony Danych procedury oraz wytyczne mające na celu przetwarzanie danych osobowych zgodnie z obowiązującym prawem.
5) Korzysta z systemu informatycznego Administratora Danych w sposób zgodny z procedurami.
6) Zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV. Przetwarzanie Danych Osobowych

1. Pomieszczenia w których przetwarza się dane osobowe

1) Pomieszczeniami tworzącymi obszar, w którym znajdują się przetwarzane dane osobowe są pomieszczenia w których znajdują się zbiory danych w formie kartotek, rejestrów i innej oraz stacjonarny sprzęt komputerowy, w którym są przetwarzane dane osobowe. Pomieszczenia te znajdują się w budynkach przy ulicy Handlowej 2 w Zabrzu (41-807).

2) Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania, osób nieuprawnionych do dostępu do danych osobowych, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.
3) Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane i chronione na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osób trzecich.

V. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności przetwarzanych danych

W Zakładzie rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   - pomieszczenia zamykane na klucz,
   - szafy zamykane na klucz,
   - budynek objęty jest całodobową kontrolą przez firmę ochroniarską,
   - wjazd na teren firmy jest możliwy po okazaniu identyfikatora lub po zarejestrowaniu na wjeździe na teren Zakładu,
   - wdrożony monitoring wizyjny, identyfikujący osoby przebywające na terenie Zakładu.
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   - przetwarzanie danych osobowych następuje w wyznaczonych obszarach,
   - przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
3. Zabezpieczenia organizacyjne:
   - osobą odpowiedzialną za bezpieczeństwo danych jest Administrator Danych Osobowych,
   - jest wyznaczony Inspektor Ochrony Danych;
   - Administrator systemów na bieżąco kontroluje pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami. Zarząd kontroluje sposób, systematyczność oraz prowadzoną dokumentację z zakresu kontroli.
4. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:
   - w Zakładzie jest stworzony rejestr osób upoważnionych, który na bieżąco jest aktualizowany,
   - przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie,

- w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
- przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,
- w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
- po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

VI. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami

Dokumenty dostarczane do firmy w formie papierowej lub drogą elektroniczną każdorazowo są analizowane pod kątem ich zgodności, akceptowane, a następnie wprowadzane do systemów przetwarzania danych.

Opisy poszczególnych pól informacyjnych w strukturze zbioru danych jednoznacznie wskazują, jakie kategorie danych są w nich przechowywane. Opis pola danych, gdy możliwa jest niejednoznaczna interpretacja jego zawartości, wskazuje nie tylko kategorię danych, ale również format jej zapisu i/lub określone w danym kontekście znaczenie.

VII. Procedura realizacji praw jednostki

1. Zakres stosowania procedury

   Niniejsza procedura ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

2. Prawa osób, których dane dotyczą

   1) Prawo dostępu do danych osobowych

   a. Osoba, której dane dotyczą jest uprawniona do uzyskania od Zakładu Mechanicznego „BUMAR-MIKULCZYCE" S.A w Zabrzu potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

- cele przetwarzania;
- kategorie odnośnych danych osobowych;
- informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- w miarę możliwości planowanych okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO oraz przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą

b. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej osoba, której dane dotyczą ma prawo poinformowania o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

c. Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A w Zabrzu dostarcza osobie, której dane dotyczą kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą Zakład może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Kopia danych osobowych przekazywana jest we wskazanym przez osobę, której dane dotyczą formacie. Jeżeli osoba, której dane dotyczą zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

d. Prawo do uzyskania kopii, o której mowa powyżej, nie może niekorzystnie wpływać na prawa i wolności innych, w szczególności na prawo do prywatności, ochrony danych osobowych, tajemnicę przedsiębiorstwa, własność intelektualną czy prawa autorskiego chroniącego oprogramowanie.

e. Uprawnienie dostępu do danych osobowych przysługuje bez względu na formę przetwarzania danych, rodzaj przetwarzanych danych czy ich archiwizacji.

2) Prawo do sprostowania danych

a. Osoba, której dane dotyczą ma prawo żądania od Zakładu Mechanicznego „BUMAR-MIKULCZYCE" S.A w Zabrzu niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Dane nieprawidłowe to dane, które nie odpowiadają rzeczywistemu stanowi rzeczy. Innymi słowy, dane nieprawidłowe to dane nieprawdziwe. Prawidłowość danych osobowych powinno się oceniać z perspektywy osoby, której dane dotyczą i badać zgodność tych danych z rzeczywistością, którą opisują. Zatem stan prawidłowości lub nieprawidłowości danych osobowych podlega ocenie obiektywnej w odniesieniu do osoby, której dane dotyczą.

b. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych. Dane niekompletne to dane, co prawda prawidłowe, ale niepełne co do swojego zakresu. Kompletność danych osobowych powinno się oceniać z punktu widzenia („z uwzględnieniem") celu przetwarzania danych, który w oparciu o zasadę minimalizacji danych osobowych wyznacza zakres przetwarzania danych. Innymi słowy stan kompletności lub niekompletności danych podlega ocenie obiektywnej w odniesieniu do celu, w którym dane są przetwarzane.

c. Jeżeli osoba, której dane dotyczą wykaże, że Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A w Zabrzu przetwarza dane nieprawidłowe lub niekompletne wówczas Zakład niezwłocznie prostuje dane nieprawidłowe lub uzupełnia dane niekompletne. Wybór jednego ze wskazanych sposobów działania powinien być dostosowany do charakteru zaistniałego i wykazanego uchybienia w procesie przetwarzania danych osobowych.

3) Prawo do usunięcia danych („prawo do bycia zapomnianym")

a. Osoba, której dane dotyczą ma prawo żądania od Zakładu Mechanicznego „BUMAR-MIKULCZYCE" S.A w Zabrzu niezwłocznego usunięcia dotyczących jej danych osobowych, a Zakład ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- dane osobowe nie są już niezbędne do celów, w którym zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit.a) lub art. 9 ust.2 lit. a) RODO, i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;

- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Zakład;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.

b. Jeżeli Zakład upublicznił dane osobowe, ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne, działania w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą żąda by administratorzy ci usunęli wszelkie łącze do tych danych, kopie tych danych osobowych lub ich replikacje.

c. Wskazane powyżej działania nie będą stosowane przez Zakład w zakresie w jakim przetwarzanie danych osobowych jest niezbędne:
- do korzystania z prawa do wolności wypowiedzi informacji
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Zakład lub do wykonania żądania realizowanego w Interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Zakładowi;
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. f) oraz i) art. 9 ust. 3 RODO;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo do usunięcia danych, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania lub;
- do ustalenia, dochodzenia lub obrony roszczeń.

4) Prawo do ograniczenia przetwarzania

a. Osoba, której dane dotyczą ma prawo żądania od Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A w Zabrzu ograniczenia przetwarzania danych w następujących przypadkach:
- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Zakładowi sprawdzić prawidłowość tych danych;
- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą sprzeciwia się usunięciu danych osobowych żądając w zamian ograniczenia ich wykorzystywania;
- Zakład nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszeń;

- osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia czy prawnie uzasadnione podstawy po stronie Zakładu są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

b. Jeżeli przetwarzanie zostało ograniczone takie dane osobowe można przetwarzać z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą lub w celu ustalenia dochodzenia lub obrony roszczeń, lub w celu ochrony prawnej innej osoby fizycznej lub prawnej lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

c. Przed uchyleniem ograniczenia przetwarzania Zakład informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

5) Prawo do przenoszenia danych

a. Osoba, której dane dotyczą ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące które dostarczył administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Zakładu, któremu dostarczono te dane osobowe jeżeli przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art.9 ust.2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO oraz przetwarzanie odbywa się w sposób zautomatyzowany.

b. Wykonując prawo do przenoszenia danych osoba, której dane dotyczą ma prawo żądania, by dane osobowe zostały przesłane przez Zakład bezpośrednio innemu administratorowi o ile jest to technicznie możliwe

c. Wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa do usunięcia danych (do bycia zapomnianym). Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Zakładowi.

d. Prawo do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych osób.

e. Prawo do przenoszenia danych nie obejmuje danych wytworzonych przez Zakład Mechaniczny „BUMAR-MIKULCZYCE” S.A w Zabrzu.

f. Prawo do przenoszenia danych znajduje zastosowanie wtedy, gdy przetwarzanie danych odbywa się w sposób zautomatyzowany, zatem nie obejmuje ono tzw. zbiorów papierowych.

g. W przypadku skorzystania z prawa do przenoszenia danych nie dochodzi do automatycznego usunięcia danych w Zakładzie Mechanicznym „BUMAR-MIKULCZYCE” S.A. Zakład nadal może przetwarzać dane osobowe, dopóki dysponuje podstawą prawną legalizującą przetwarzanie tj. zgodą osoby, której dane dotyczą, bądź, gdy są one niezbędne do wykonania umowy.

6) Prawo do sprzeciwu

a. Osoba, której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją. Administrator nie może już przetwarzać tych danych osobowych, chyba, że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów praw i wolności osoby, której dane dotyczą lub podstaw do ustalenie dochodzenia lub obrony roszczeń.

b. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą wyraźnie informuje się ją o prawie do sprzeciwu oraz przedstawia się je jasno i odrębnie od wszelkich innych Informacji.

c. Sprzeciw nie wymaga uzasadnienia i może zostać wniesiony pisemnie lub elektronicznie.

d. W razie otrzymania sprzeciwu wobec przetwarzania danych osobowych ze względu na szczególną sytuację osoby, której dane dotyczą, Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A w Zabrzu powinien niezwłocznie zaprzestać przetwarzania danych, jeżeli uzna sprzeciw za zasadny. Jeżeli Zakład uzna sprzeciw za pozbawiony podstaw w szczególności z takiej przyczyny, że w jego ocenie nie zachodzi szczególna sytuacja uzasadniająca wniesienia sprzeciwu lub w ocenie Zakładu istnieją ważne prawnie uzasadnione podstawy do przetwarzania nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą lub podstawy do ustalenia, dochodzenia lub ochrony roszczeń administrator może nadal przetwarzać dane objęte sprzeciwem. Jeżeli osoba, której dane dotyczą nie zgadza się z taką oceną zaistniałej sytuacji, może skorzystać z prawa do wniesienia skargi do organu nadzorczego.

7) Zasady postępowania i terminy realizacji praw przysługujących osobie, której dane dotyczą

Sposób realizowania praw jednostki

a. Uprawnienia wynikające z niniejszej procedury mogą być realizowane przez osobę, której dane dotyczą zarówno osobiście jak i przez przedstawiciela ustawowego czy pełnomocnika

b. W przypadku zgłoszenia żądania drogą pisemną, w tym w szczególności, gdy żądanie zostanie zaadresowane jest na adres Zakładu Mechanicznego „BUMAR-MIKULCZYCE" S.A w Zabrzu, żądanie przekazywane jest niezwłocznie przez odpowiedni personel Zakładu do Inspektora Ochrony Danych

Weryfikacja tożsamości wnioskodawcy

a. Zakład nie odmawia podjęcia działań na żądanie osoby, której dane dotyczą pragnącej wykonać prawa wynikające z niniejszej procedury. Zakład może odmówić podjęcia

działań w sytuacji, kiedy wykaże, że nie jest w stanie zidentyfikować osoby, której dane dotyczą.

b. Zakład sprawdza tożsamość osoby fizycznej składającej żądanie realizacji sowich praw o tórych mowa w niniejszej procedurze poprzez żądanie przekazania informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. W przypadku powzięcia wątpliwości, co do tożsamości wnioskodawcy, Zakład zastrzega sobie prawo do przeprowadzenia pogłębionego uwierzytelnienia, w postaci żądania dodatkowego pytania z akt osobowych pracownika o dużym stopniu personalizacji np. podanie nazwiska panieńskiego matki lub podania imion rodziców. Przedmiotowe weryfikacja ma na celu umożliwiać przekazanie informacji podmiotom nieuprawnionym.

Weryfikacja kompletności wniosku lub przesłanek wyłączających możliwość jego rozpoznania

a. Po zweryfikowaniu tożsamości osoby Zakład dokonuje weryfikacji przedmiotu wniosku pod kątem jego kompletności oraz czy wniosek nie jest nadmierny lub ewidentnie nieuzasadniony. W przypadku stwierdzenia braku wystarczających danych osobowych lub nadmierności wniosku lub jego ewidentnej niezasadności Zakład odmawia rozpoznania wniosku, o czym informuje wnioskodawcę wraz z pouczeniem o możliwości wniesieniu skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem oraz wyjaśnieniem przyczyn odmowy rozpoznania wniosku. W tej sytuacji gdy przyczyną odmowy rozpoznania wniosku jest brak odpowiednich danych lub konkretyzacji żądania, w wyjaśnieniu Zakład informuje jakich danych zabrakło do rozpoznania wniosku.

Udzielenie odpowiedzi dla wnioskodawcy

a. Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A w Zabrzu udziela informacji na piśmie lub w inny sposób, w tym stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą tego zażąda informacji można udzielić ustnie o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

b. Zakład informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdemu odbiorcy, któremu ujawniono dane osobowe, chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Zakład informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą tego żąda.

Termin realizacji praw jednostki

a. Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A w Zabrzu bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od pozytywnej weryfikacji tożsamości wnioskodawcy, udziela osobie, której dane dotyczą informacji o działaniach podjętych

w związku z żądaniem. W razie potrzeby termin ten można przedłożyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Zakład informuje osobę, której dane dotyczą o takim przedłużeniu terminu z podaniem przyczyn opóźnienia.

Prawo do skargi

a. Jeżeli Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A w Zabrzu nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę której dane dotyczą o powodach niepodjęcia działań oraz możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Możliwość ustalenia opłaty

a. Informacje oraz komunikacja i działania podejmowane w przedmiocie realizacji praw jednostki są co do zasady wolne od opłat. Jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Zakład może:

- pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji prowadzenia komunikacji lub podjęcia żądanych działań; albo
- odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na Zakładzie Mechanicznym „BUMAR-MIKULCZYCE" S.A w Zabrzu.

2. Obowiązek informacyjny

a. Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A w Zabrzu podczas pozyskiwania danych osobowych podaje wszystkie następujące informacje:

- swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
- dane kontaktowe Inspektora Ochrony Danych;
- cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz stwierdzeniu braku lub braku stwierdzenia przez Komisję odpowiedniego

stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub miejscu udostępnienia danych.

b. Poza informacjami, o których mowa powyżej podczas pozyskiwania danych osobowych Zakład podaje następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
   - okres, przez który dane będą przechowywane, a gdy nie jest to możliwe, kryteria ustania tego okresu;
   - informacje o prawie do żądania od Zakładu dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   - jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   - informacje o prawie wniesienia skargi do organu nadzorczego;
   - informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
   - informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

c. Jeżeli Zakład planuje przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosowanych informacji, o których mowa w pkt. a oraz b.

d. Zasady wskazane powyżej nie mają zastosowania, gdy w zakresie, w jakim osoba, której dane dotyczą dysponuje już tymi informacjami.

VIII. Kontrola wewnętrzna stanu ochrony danych osobowych i przestrzegania zasad ich ochrony

1. Inspektor Ochrony Danych sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2. Inspektor Ochrony Danych sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych. Inspektor Ochrony Danych dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
3. Zaobserwowane błędy oraz zaniechania w przestrzeganiu zasad określonych w dokumentacji dotyczącej ochrony danych osobowych przedstawia się Administratorowi Danych Osobowych oraz pracownikom upoważnionym do przetwarzania danych osobowych.

IX. Szkolenia lub zapoznawanie osób z zasadami ODO

1. Każda osoba przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami w wersji papierowej winna być poddana przeszkoleniu lub zapoznana z:
   1) podstawami prawnymi dotyczącymi bezpieczeństwa danych osobowych,
   2) zasadami ochrony danych osobowych zawartymi w Polityce.
2. Za przeprowadzenie szkolenia lub zapoznania z zasadami ochrony danych osobowych odpowiada osoba wyznaczona przez Administratora Danych Osobowych.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą listy obecności z przeprowadzonego szkolenia.
4. Każda nowozatrudniona osoba po odbytym szkoleniu lub po zapoznaniu z zasadami ochrony danych osobowych zobowiązana jest do podpisania Zobowiązania do zachowania poufności.
5. Podpisane Zobowiązania zostają zarchiwizowane, w aktach osobowych lub teczkach pracowników.

X. Praca zdalna w związku z sytuacją pandemiczną wywołaną koronawirusem SARS-CoV-2

1. Pracownik może korzystać z papierowej dokumentacji zawierającej dane osobowe wyłącznie za zgodą pracodawcy. Obszar przetwarzania takich danych musi być jasno określony przez przełożonego.

2. Administratorem danych osobowych przetwarzanych przez pracowników podczas pracy zdalnej jest pracodawca. Na pracodawcy spoczywa obowiązek zapewnienia przestrzegania zasad bezpieczeństwa danych, zarówno tych przetwarzanych za pośrednictwem urządzeń elektronicznych, jak i zawartych w dokumentacji papierowej.

3. Pracownik może przetwarzać dane osobowe wyłącznie w związku
z wykonywaniem powierzonych mu obowiązków służbowych,
z zachowaniem ustalonej przez pracodawcę polityki bezpieczeństwa i procedur w tym zakresie.

4. Pracodawca powierzając wykorzystywanie dokumentacji papierowej podczas pracy zdalnej winien spełnić następujące warunki:

a) zadbać o ewidencjonowanie powierzonej dokumentacji zawierającej dane osobowe,

b) zapewnić ograniczone przechowywanie materiałów — papierowe dokumenty
z danymi osobowymi mają być przechowywane przez pracownika wyłącznie na czas wykonywania określonego zadania czy projektu,

c) ograniczenie liczby dokumentów, które zdalny pracownik wynosi z siedziby administratora — powierzona dokumentacja ma być niezbędna do celu przetwarzania danych osobowych przez pracownika,

d) przenoszone dokumenty muszą być odpowiednio zabezpieczone, np.
w zabezpieczonej teczce, zamykanej na kod walizce, w sposób niewidoczny dla osób trzecich,

e) dokumenty muszą być również odpowiednio zabezpieczone w miejscu wykonywania pracy zdalnej, np. w szafkach i biurkach zamykanych na klucz, w miejscach niedostępnych dla nieuprawnionych osób trzecich, np. członków rodziny pracownika,

f) zapewnienie, aby pracownik wykorzystywał powierzoną dokumentację wyłącznie
w tym celu, w jakim byłaby ona wykorzystywana w stałym miejscu pracy,

g) ustalenie procedury niszczenia dokumentów, np. zakaz wyrzucania ich do domowego kosza, konieczność odpowiedniego zabezpieczenia w celu zniszczenia ich po zakończonym projekcie (np. rekrutacja) w niszczarce znajdującej się w biurze — jeśli pracownik nie ma w domu takiego sprzętu, pracodawca ma obowiązek poinstruowania pracownika o konieczności zgłoszenia każdego incydentu naruszenia bezpieczeństwa danych osobowych. Pracodawca jako administrator danych musi
w takiej sytuacji wywiązać się z obowiązku, o którym mowa w artykule 33 ust. 1 Rozporządzenia RODO (zgłoszenie naruszenia danych osobowych organowi nadzorczemu nie później niż w terminie 72 godzin po stwierdzeniu incydentu).

Jeśli nie jest możliwe zastosowanie wyżej wymienionych rozwiązań, należy rozważyć pracę na kopiach dokumentów zawierających dane osobowe, a pracownik ma obowiązek chronić na równi dane osobowe zawarte w kopii i oryginalnym dokumencie.

5. Pracownik nie powinien przenosić dokumentacji papierowej z biura do miejsca wykonywania pracy zdalnej w następujących przypadkach:

a) pracodawca wdrożył elektroniczny obieg dokumentów, więc pracownik ma bezpieczny dostęp do niezbędnych danych osobowych za pośrednictwem środków komunikacji elektronicznej,

b) pracodawca może udostępnić zdalnemu pracownikowi odpowiednio zaszyfrowane elektroniczne kopie dokumentów zawierających dane osobowe,

c) pracodawca może szybko i bezpiecznie wdrożyć elektroniczny obieg dokumentacji w firmie.

6. Pracodawca ma obowiązek każdorazowo ocenić niezbędność wykorzystania przez zdalnego pracownika papierowej dokumentacji zawierającej dane osobowe. W tym celu musi uwzględnić dostępne środki, charakter danych oraz cele, dla których te dane są przetwarzane.

7. Przyjmowane rozwiązania pracy zdalnej muszą już w fazie ich projektowania być zgodne z rozporządzeniem RODO – zasada privacy by design (art. 25 rozporządzenia RODO).

8. Należy zapewnić każdemu z pracowników odpowiednie szkolenie
z zakresu obowiązującej w firmie procedury bezpieczeństwa oraz zasad korzystania
z narzędzi i również zadbać o udokumentowanie tego faktu.

9. Dział Kadr wdroży oświadczenia o zachowaniu poufności oraz upoważnienia do przetwarzania danych osobowych, jak również sam rejestr takich upoważnień dla określonych osób wykonujących pracę zdalną. .

10. Pracodawcy, biorąc pod uwagę zawodowy charakter ich działalności i obowiązek dołożenia należytej staranności, uregulują kwestie pracy zdalnej
w dokumentacji wewnętrznej tj. wdrożyć regulamin pracy zdalnej.

11. Pracodawca, przy pomocy określonej komórki organizacyjnej sporządzi ewidencję urządzeń przenośnych, które mają dostęp do danych firmowych.

12. Pracodawca będzie ewidencjonować pozyskane zgody na przetwarzanie danych osobowych np. w formie ewidencji zgód.

13. Pracodawca powinien przypominać pracownikom o konieczności dopełniania obowiązku informacyjnego wobec klientów, kontrahentów np. w formie komunikatu lub instrukcji zgodnie z art. 24 ust. 2 rozporządzenia RODO, który przewiduje obowiązek wdrożenia polityk ochrony danych osobowych, gdy jest to proporcjonalne w stosunku do czynności przetwarzania.

14. Konieczność pracy zdalnej i związane z tym ryzyka i wyzwania w zakresie ochrony danych osobowych stanowią o podstawie do samoregulacji przez Administratorów danych osobowych.

XI. Postanowienia końcowe

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom i instytucjom postronnym w żadnej formie bez zgody ADO oraz IOD.
2. Polityka Bezpieczeństwa może być udostępniania osobom i instytucjom postronnym bez zgody ADO oraz IOD, jeżeli nie zawiera w treści informacji o zabezpieczeniach danych osobowych, a wszelkie załączniki występują w formie niewypełnionych szablonów.
3. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszej Polityce.
4. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
5. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy 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) oraz wydanych na jej podstawie aktów wykonawczych.
6. Zmiana dokonana w załączniku do niniejszej Polityki powoduje aktualizację danego załącznika, nie powoduje natomiast zmiany całości dokumentu. Po dokonaniu aktualizacji załącznika jego wcześniejsza wersja automatycznie traci ważność.

XII. Załączniki

Nr 1– Instrukcja Zarządzania Systemem Informatycznym