HUT-PUS Spółka Akcyjna
31-752 Kraków, ul. Mrozowa 1
tel. 12 643 87 04
NIP 678-002-62-01 REGON 350035148

ZARZĄDZENIE Nr 2/2018

Prezesa Zarządu HUT-PUS S.A.
z dnia 17 maja 2018 roku

w sprawie: polityki bezpieczeństwa przetwarzania danych osobowych.

W celu zapewnienia, że dane osobowe będą przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczania danych, w tym przede wszystkim z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO),

zarządzam:

§ 1

Z dniem 25.05.2018 roku wprowadzam w życie „Politykę Bezpieczeństwa przetwarzania danych osobowych" w HUT-PUS S.A. z siedzibą w Krakowie, ul. Mrozowa 1" – stanowiącą załącznik do niniejszego Zarządzenia.

§ 2

Celem „Polityki Bezpieczeństwa przetwarzania danych osobowych" jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Spółce informacji zawierających dane osobowe.

§ 3

Zgodnie z „Polityką Bezpieczeństwa przetwarzania danych osobowych", wyznaczam następujące osoby do nadzorowania przestrzegania w/wym. zasad, każdy w swoim zakresie:

I. Administrator Danych Osobowych (ADO) - Pani Anna Karpierz
II. Inspektor Ochrony Danych (IOD) - Pani Jolanta Urynowicz
III. Administrator Systemów Informatycznych (ASI) - Pan Paweł Janik

§ 4

Kierujący komórkami organizacyjnymi spółki przekażą podległym pracownikom do wiadomości i stosowania zasady Polityki Bezpieczeństwa.

§ 5

Nadzór nad realizacją niniejszego Zarządzenia sprawuje Szef Biura Zarządu.

§ 6

1. Zarządzenie wchodzi w życie z dniem 25 maja 2018 r.

2. Zarządzenie zastępuje zarządzenie z dnia 30.12.2014 r. numer 8/2014 w sprawie polityki bezpieczeństwa informacji.

Załącznik – Polityka Bezpieczeństwa Informacji

Rozdzielnik:
Wszystkie komórki organizacyjne spółki

Prezes Zarządu HUT-PUS S.A.
PREZES ZARZĄDU
mgr Tomasz Karpierz

Załącznik nr 1 do Zarządzenia Prezesa Z-du
Nr 2/2018 z dnia 17 maja 2018 r.

Polityka Bezpieczeństwa danych osobowych w HUT-PUS S.A. (Instrukcja)

Spis treści:

Niniejsza *polityka bezpieczeństwa*, zwana dalej Polityką, została sporządzona w celu zagwarantowania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczania danych, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO).

I. Postanowienia ogólne

§1

1. Polityka Bezpieczeństwa Informacji, zwana dalej Polityką, określa zakres oraz zasady prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
2. Niniejszy dokument opisuje reguły bezpieczeństwa przetwarzania danych osobowych w sposób tradycyjny (w formie papierowej) oraz w systemach informatycznych.
3. Opisane reguły określają granice dopuszczalnego zachowania wszystkich pracowników biorących udział w przetwarzaniu danych osobowych.
4. Polityka bezpieczeństwa określa tryb postępowania w przypadku:
   - stwierdzenia naruszenia zabezpieczenia systemu informatycznego,
   - stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy,
   - sposób działania programu lub jakość komunikacji w sieci informatycznej może wskazywać na naruszenie zabezpieczenia tych danych.
5. Polityka bezpieczeństwa obowiązuje wszystkich pracowników HUT-PUS S.A w Krakowie ul. Mrozowa 1.
6. Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, między innymi poprzez należyty dobór zakresu oraz metod przetwarzania danych, jak i stosowanych środków ochrony, właściwą ocenę, udokumentowanie oraz zgłaszanie przypadków naruszenia danych, kontrolę i nadzór nad przetwarzaniem danych, monitorowanie zastosowanych środków ochrony, jak również kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji.
7. Polityka jest przechowywana w wersji elektronicznej oraz papierowej w siedzibie Administratora Danych Osobowych i jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.

§2

1. Polityka Bezpieczeństwa Informacji zastępuje dotychczasowe akty wewnętrzne dotyczące ochrony danych osobowych, to jest Zarządzenie Prezesa Z-du Nr 8/2014 z dnia 30 grudnia 2014 r. wraz z załącznikami.
2. Niniejszy dokument opracowano na podstawie:
   - ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
   - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

   - w celu zapewnienia wykonania postanowień tych aktów prawnych.

§3

Użyte w Polityce Bezpieczeństwa Informacji określenia oznaczają:

1. ustawa - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),

2. rozporządzenie, a także RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

3. dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

4. zbiór danych osobowych – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów,

5. przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane w jakikolwiek sposób na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, raportowanie, aktualizowanie, archiwizowanie, udostępnianie i usuwanie,

6. system informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

7. **bezpieczeństwo systemu informatycznego** – środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, modyfikacją, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,

8. instrukcja – instrukcja zarządzania systemem informatycznym,

9. Administrator Danych Osobowych (ADO) - „Hut - Pus" Spółka akcyjna z siedzibą w Krakowie, ul. Mrozowa 1, 31 – 752 Kraków, numer KRS: 0000055658, REGON: 350035148, NIP: 6780026201, w imieniu której czynności ADO będzie wykonywać Prezes Zarządu lub osoba przez niego wskazana,

10. osoba upoważniona lub użytkownik systemu - osoba posiadająca upoważnienie wydane przez ADO lub osobę przez niego uprawnioną, dopuszczona jako użytkownik do przetwarzania danych osobowych, w zakresie wskazanym w upoważnieniu,

11. osoba uprawniona - osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności,

12. identyfikator użytkownika (login) - ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

13. logowanie - uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika;

14. **hasło** (password) - ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie upoważnionej do pracy w systemie informatycznym.

§4

1. Dane osobowe muszą być:
   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 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do

celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 Rozporządzenia, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy Rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania");

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").

2. Postanowienia niniejszej Polityki mają na celu zagwarantowanie bezpieczeństwa przetwarzanych danych już w fazie projektowania oraz zapewnienie Administratorowi możliwości wykazania przestrzegania zasad opisanych w ustępie pierwszym ("rozliczalność").

§5

Celem wdrożenia Polityki Bezpieczeństwa jest ochrona zbiorów danych osobowych, w tym ochrona systemów informatycznych jako całości i jego poszczególnych elementów, przetwarzanych przez systemy zbiorów danych, obszaru, w którym przetwarzane są dane osobowe, a przede wszystkim zapewnienie technicznych i organizacyjnych uwarunkowań mających wpływ na zarządzanie zbiorami danych osobowych.

Polityka Bezpieczeństwa w HUT-PUS S.A. polega na:

1. działaniu zgodnym z przepisami prawa,
2. zapobieganiu uzyskania dostępu do danych osobowych przez osoby nieupoważnione,
3. określeniu procedur postępowania w przypadku naruszenia zasad niniejszego dokumentu, zgłaszania przypadków naruszeń oraz konsekwencji ponoszonych przez osoby naruszające,
4. ustaleniu i odpowiednim zabezpieczeniu pomieszczeń lub ich części tworzących obszar, w którym są przetwarzane dane,
5. podnoszeniu świadomości pracowników mających dostęp do przetwarzanych danych osobowych w Spółce.

Zarządzanie bezpieczeństwem danych osobowych realizowane jest w szczególności przez zapewnienie przez kierownictwo warunków umożliwiających realizację i egzekwowanie następujących działań:

1) utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację,
2) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,
3) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji,
4) bezzwłoczne zmiany uprawnień, w przypadku zmiany zadań, o których mowa w pkt. 3,
5) zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji,
6) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą,
7) ustanowieniu podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
8) bezzwłocznego zgłaszania incydentów naruszenia zgodnie z RODO bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących,

9) zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

III. Zakres oraz zasady przetwarzania danych osobowych

§6

1. Administrator przetwarza dane osobowe w systemach informatycznych oraz w formie papierowej w celu wykonywania zadań określonych profilem prowadzonej przez siebie działalności gospodarczej, w tym przede wszystkim zadań HUT-PUS S.A. jako pracodawcy.
2. Informacje, o których mowa w ust. 1 są przetwarzane i składowane zarówno w postaci papierowej jak i elektronicznej.
3. Dla każdego z zadań, w ramach których możliwe jest przetwarzanie danych osobowych nakazuje się gromadzenie tylko tych danych osobowych, które są niezbędne do realizacji celu, w związku z którym dane są przetwarzane, przy czym przez realizację celu rozumieć należy przede wszystkim spełnienie wymogów stawianych przez powszechnie obowiązujące prawo oraz zakres, cel i gwarancję wykonania umów, których HUT-PUS S.A. jest stroną. Dane osobowe powinny być przechowywane przez możliwie krótki czas, z poszanowaniem jednak interesów, praw i obowiązków HUT-PUS S.A. oraz jej kontrahentów.

§7

1. Przetwarzanie danych osobowych nie może naruszać praw i wolności osób, których dane osobowe dotyczą, a w szczególności zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, z zastrzeżeniem ust. 2.
2. Dane dotyczące przynależności do związków zawodowych, dane o ukaraniu, w tym także mandatami karnymi, dane ujawniające pochodzenie rasowe lub etniczne oraz dane o stanie zdrowia mogą być przetwarzane w zakresie, w jakim wynika to z obowiązków nałożonych na ADO przez przepisy powszechnie obowiązującego prawa, zwłaszcza w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej lub w wypadku wyraźnej zgody osoby, której dane dotyczą, w celu realizacji konkretnego celu, wskazanego przez tę osobę w oświadczeniu o wyrażeniu zgody na przetwarzanie danych, a także w innych wypadkach wyraźnie wskazanych w przepisach powszechnie obowiązującego prawa.

§8

1. Przetwarzanie danych osobowych jest dopuszczalne wyłącznie do celów wynikających z obowiązujących przepisów prawa z zastrzeżeniem ust. 2.
2. Przetwarzanie danych osobowych w innym celu jest dopuszczalne, gdy przepis prawa tak stanowi lub osoba, której dane dotyczą wyrazi na to zgodę.

§9

Dane osobowe mogą być uzyskiwane:
1. bezpośrednio od osób, których te dane dotyczą.
2. z innych źródeł, w granicach dozwolonych przepisami prawa.

§10

1. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, osoba zbierająca dane osobowe jest zobowiązana, zgodnie z ustawą, poinformować tę osobę o:
   a) celach przetwarzania danych osobowych, oraz podstawie prawnej przetwarzania;
   b) informacji o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   c) gdy ma to zastosowanie - informacji o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu 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 Rozporządzenia, wzmiance o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
   d) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   e) prawie do żądania od administratora 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;
   f) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) Rozporządzenia - o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   g) prawie wniesienia skargi do organu nadzorczego;
   h) 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;
   i) 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 – jeżeli ma to zastosowanie.
2. Jeżeli planowane jest dalsze przetwarzanie danych osobowych w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem należy poinformować osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.
3. Obowiązek informacyjny, o którym mowa w ust. 1, powinien być wykonany w momencie zbierania danych. Jest on jednak wyłączony gdy:
   a. przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,
   b. osoba, której dane dotyczą, posiada już informacje o których mowa w ust. 1 i 2. (Jeżeli dochodzi do ponownego zbierania danych (przez tego samego administratora, do tych samych celów), można powołać się na spełniony już wcześniej obowiązek poinformowania.)
4. Wzór formularza stosowanego dla spełnienia obowiązków wymienionych w ust. 1 i 2, o ile nie gwarantują spełnienia tego obowiązku inne formularze wypełniane i podpisywane przez zainteresowaną osobę, określa załącznik Nr 1 do niniejszej Polityki.
5. Formularze stosowane w HUT-PUS S.A. od dnia wejścia w życie Polityki muszą odpowiadać powyższym wymogom, zatem zadaniem pracowników – każdego w zakresie jego kompetencji – jest czuwanie, aby obowiązek informacyjny wobec osoby, której dane dotyczą, był realizowany zgodnie z niniejszym paragrafem oraz pozostałymi przepisami Polityki.

§11

1. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy poinformować ponadto, co wynika z § 10, także o:
   1) źródle danych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych;
   2) kategorie odnośnych danych osobowych.
2. Wzór formularza stosowanego dla spełnienia obowiązków wymienionych w ust. 1, o ile nie gwarantują spełnienia tego obowiązku inne formularze wypełniane i podpisywane przez zainteresowaną osobę, określa załącznik Nr 2 do niniejszej Polityki.

§12

1. Przetwarzanie danych osobowych może zostać powierzone innemu podmiotowi, wyłącznie w celu określonym w § 8, pod warunkiem zawarcia z tym podmiotem pisemnej umowy zgodnie z przepisami prawa.
2. HUT-PUS S.A. posługuje się wzorem umowy powierzenia określonej odrębnym zarządzeniem, przy czym relacje z poszczególnymi kontrahentami mogą uzasadniać zastosowanie innego wzorca umowy. Za każdym jednak razem należy przestrzegać dbałości o to, by umowa taka odpowiadała zasadom bezpieczeństwa przetwarzania danych osobowych obowiązujących w HUT-PUS S.A.

§13

Każdej osobie, której dane osobowe są przetwarzane przysługuje zgodnie z ustawą prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych.

§14

1. Na wniosek osoby, której dane osobowe dotyczą IOD jest zobowiązany niezwłocznie, nie później jednak, niż w terminie 30 dni od dnia wpłynięcia wniosku, poinformować o przysługujących jej prawach oraz udzielić odnośnie jej danych osobowych informacji zgodnie z zakresem określonym w Rozporządzeniu.
2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie. Wzór formularza informacji określa załącznik Nr 3 do niniejszej Polityki.
3. Udzielenie informacji, o których mowa w ust. 1, w formie ustnej jest możliwe tylko w rozmowie bezpośredniej z osobą, której dane dotyczą, po sprawdzeniu jej tożsamości poprzez wylegitymowanie dokumentem tożsamości, chyba że osoba ta jest osobiście znana udzielającemu informacji.

§15

1. W razie oświadczenia przez osobę, której dane osobowe dotyczą, że jej dane osobowe są niekompletne, nieaktualne, nieprawdziwe, lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, w jakim zostały zebrane, Spółka jest zobowiązana do podjęcia wszelkich działań w celu weryfikacji tego oświadczenia, a w ich konsekwencji uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych osobowych lub ich usunięcia, zgodnie z żądaniem osoby, której dane osobowe dotyczą.
2. Na żądanie osoby, której dane dotyczą dane osobowe są przenoszone, tj. przekazywane podmiotowi wskazanemu przez uprawnionego.

§16

1. ADO udostępnia dane osobowe przetwarzane w zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa lub wiążących HUT-PUS S.A. umów, o ile udostępnienie takie odpowiada prawu.
2. O ile wiążące umowy lub przepisy prawa nie przewidują innych zasad dane osobowe udostępnia się na pisemny, umotywowany wniosek. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
3. Wnioski o udostępnienie danych osobowych przetwarzanych są rozpatrywane przez ADO, IOD lub osoby upoważnione.
4. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe nie mające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§17

Nieuprawnione ujawnienie danych osobowych może narazić na szkodę prawnie chroniony interes osób, których te dane dotyczą, zatem dane te są objęte tajemnicą służbową zgodnie z art. 2 ustawy o ochronie informacji niejawnych.

§18

1. Zasady określone w Polityce Bezpieczeństwa mają zastosowanie do wszelkich sposobów przetwarzania danych osobowych, w tym całego systemu informacyjnego, w szczególności do:
1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
2) informacji będących własnością Spółki lub klientów Spółki, o ile zostały przekazane na podstawie umów,
3) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
4) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów, praktykantów, konsultantów i innych osób mających dostęp do informacji podlegających ochronie.

2. Przy podejmowaniu się przez HUT-PUS S.A. nowych działań wiążących się z przetwarzaniem danych osobowych osoby wskazane przez ADO zobowiązane są przeprowadzić analizę ryzyka, uwzględniającą ocenę, czy obowiązujące dotychczas zasady przetwarzania danych osobowych są wystarczające i adekwatne do zapewnienia ich maksymalnej ochrony z perspektywy wdrażanego działania.

III. Obowiązki Administratora Danych Osobowych

§19

1. Do obowiązków Administratora Danych Osobowych należy w szczególności:
1) nadzór ogólny nad realizacją przepisów wynikających z ustawy,
2) zapewnienie środków technicznych i organizacyjnych gwarantujących ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy i Rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
3) opracowanie dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
4) nadawanie upoważnień do przetwarzania danych osobowych,
5) organizowanie szkoleń w zakresie przetwarzania danych osobowych i sposobów ich ochrony,

6) prowadzenie rejestru czynności przetwarzania danych,
7) zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
8) monitorowanie zastosowanych środków ochrony.
2. Administrator Danych Osobowych może powierzyć wykonywanie swoich zadań.

IV. Obowiązki Inspektora Ochrony Danych

§20

1. Inspektor Ochrony Danych w szczególności:
1) odpowiada za realizację zadań wynikających z ustawy, Polityki Bezpieczeństwa, instrukcji zarządzania systemem informatycznym i innych przepisów szczegółowych,
2) sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
3) określa we współpracy z ASI strategię zabezpieczania systemów informatycznych Spółki,
4) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Spółki,
5) sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,
6) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych,
7) sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
8) opiniuje wnioski o przyznanie danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,
9) powiadamia ASI o konieczności utworzenia identyfikatora użytkownika w systemie oraz nadaniu /zmianie /utracie uprawnień dostępu użytkownika do systemu,
10) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych,
11) realizuje szkolenia z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przy przetwarzaniu danych w systemach informatycznych,
12) prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
13) prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych,
14) prowadzi rejestr przetwarzania (dotyczy danych przetwarzanych metodą tradycyjną lub w systemach informatycznych),
15) przeprowadza co najmniej raz na rok, w terminie uzgodnionym z ADO, kontrolę w zakresie przestrzegania przez użytkowników Polityki Bezpieczeństwa, instrukcji zarządzania systemem informatycznym oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego sporządza odpowiedni raport,
16) bada ewentualne naruszenia w systemie zabezpieczeń danych osobowych,
17) sporządza raporty z naruszenia bezpieczeństwa systemu informatycznego.
2. W przypadku nieobecności Inspektora Ochrony Danych jego zadania realizuje osoba wyznaczona i upoważniona przez ADO, która składa IOD relację z działań podejmowanych w czasie jego zastępstwa.

V. Obowiązki Administratora Systemu Informatycznego

§21

1. Administrator Systemu Informatycznego jest odpowiedzialny w szczególności za:

1) wdrażanie nowych systemów informatycznych,
2) nadzorowanie poprawności przetwarzania danych,
3) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
4) optymalizację wydajności systemu informatycznego, baz danych,
5) instalację i konfigurację sprzętu sieciowego i serwerowego,
6) instalację i konfigurację oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
7) konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
8) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego,
9) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
10) zarządzanie kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
11) przyznawanie ściśle określonych praw dostępu do informacji w danym systemie,
12) zarządzanie licencjami oraz procedurami ich dotyczącymi,
13) prowadzenie profilaktyki antywirusowej,
14) sprawowanie nadzoru nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
15) sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, zlecanymi firmom zewnętrznym,
16) sprawowanie nadzoru nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, palmtopach na których przetwarzane są dane osobowe,
17) monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
18) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
19) identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Spółki,
20) określanie potrzeb w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
21) wnioskowanie do ADO w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
22) podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych.

2. W przypadku nieobecności Administratora Systemu Informatycznego jego zadania realizuje osoba wyznaczona i upoważniona przez ADO, która składa ASI relację z działań podejmowanych w czasie jego zastępstwa.

VI. Rejestracja zbiorów danych osobowych

§22

Kierownicy komórek organizacyjnych, w których przetwarzane są dane osobowe, są zobowiązani do zgłoszenia ADO informacji na temat:
1) planowanego założenia nowych zbiorów danych osobowych,
2) wnoszonych zmian do zbiorów już prowadzonych.

VII. Zabezpieczenie danych osobowych

§23

1. Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby upoważnione przez ADO lub IOD. Wzór upoważnienia oraz wzór odwołania upoważnienia stanowią załączniki nr 4 i 5 do niniejszej Polityki.

2. Prowadzi się rejestr osób upoważnionych do przetwarzania danych osobowych.
3. Rejestr, o którym mowa w ust. 2 zawiera następujące informacje:
   1) imię i nazwisko osoby upoważnionej,
   2) datę nadania uprawnień,
   3) zakres upoważnienia do przetwarzania danych osobowych,
   4) identyfikator użytkownika (osoby upoważnionej) do przetwarzania danych osobowych w systemie informatycznym,
   5) datę odebrania uprawnień,
   6) podpis użytkownika.
4. W przypadku zlecenia osobom lub podmiotom zewnętrznym wykonania usługi, z którą wiąże się konieczność zapewnienia dostępu do danych osobowych, w tym do systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania danych osobowych, ADO lub IOD powinien wydać stosowne upoważnienie. Wzór upoważnienia określa załącznik nr 6 do niniejszej Polityki.
5. ADO zbiera, ewidencjonuje i przechowuje oświadczenia osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność oraz stosowanych przy przetwarzaniu danych osobowych środkach bezpieczeństwa. Wzór oświadczenia stanowi załącznik nr 7 do niniejszej Polityki.

§24

1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają szkoleniu podstawowemu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących zasad ochrony danych osobowych określonych w Polityce Bezpieczeństwa, instrukcji zarządzania systemem informatycznym i innych przepisach szczegółowych.
2. Szkolenie, o którym mowa w ust 1, prowadzi osoba wyznaczona przez ADO.
3. Osoba upoważniona do przetwarzania danych osobowych potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz Polityką Bezpieczeństwa, instrukcją zarządzania systemem informatycznym i innymi przepisami szczegółowymi poprzez złożenie stosownego oświadczenia.

§26

1. Za bezpieczeństwo informacji odpowiedzialni są wszyscy pracownicy Spółki i inne osoby upoważnione do przetwarzania danych.
2. Wszyscy pracownicy Spółki i inne osoby upoważnione do przetwarzania danych, pod groźbą sankcji dyscyplinarnych i karnych, mają obowiązek zachowania w tajemnicy informacji o przetwarzanych danych osobowych oraz o stosowanych sposobach ich zabezpieczeń. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia łub współpracy.

§27

Użytkownicy są w szczególności zobowiązani do:
1) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji, określonych w Polityce Bezpieczeństwa i instrukcji zarządzania systemem informatycznym oraz innych procedurach dotyczących zarządzania bezpieczeństwem informacji,
2) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach),
3) zabezpieczania zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce Bezpieczeństwa, instrukcji zarządzania systemem informatycznym i innych procedurach dotyczących zarządzania bezpieczeństwem informacji,

4) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie,
5) nieudzielania informacji o danych osobowych przetwarzanych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione,
6) niezwłocznego zawiadamiania swojego bezpośredniego przełożonego, a gdy dotyczy to danych utrwalonych w zbiorach informatycznych również ASI, o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych.

§28

Do obowiązków kierowników komórek organizacyjnych należy w szczególności:
1) sprawowanie bezpośredniego nadzoru nad stosowaniem środków organizacyjnych i technicznych zapewniających ochronę przetwarzania danych w podległych komórkach organizacyjnych,
2) identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone może być przetwarzanie danych osobowych,
3) informowanie na piśmie ADO o potrzebach i usprawnieniach w zakresie zabezpieczeń danych osobowych w podległych komórkach organizacyjnych,
4) niezwłoczne zawiadamianie ADO, IOD a gdy dotyczy to danych utrwalonych w zbiorach informatycznych również ASI, o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych.

§29

Stosowane środki organizacyjne i techniczne niezbędne dla zapewnienia poufności, dostępności i integralności przetwarzania danych osobowych określa załącznik nr 12 do niniejszej Polityki.

VIII. Kontrola nad przestrzeganiem ochrony danych osobowych

§30

1. Bieżącą kontrolę nad przetwarzaniem danych osobowych sprawuje IOD, a odnośnie danych przetwarzanych w systemach informatycznych także ASI.

§31

1. Na polecenie ADO co najmniej raz na rok prowadzi się kontrolę w zakresie przestrzegania przez użytkowników Polityki Bezpieczeństwa, instrukcji zarządzania systemem informatycznym oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego może być sporządzony odpowiedni raport.
2. Do przeprowadzenia kontroli, o której mowa w ust 1, ADO upoważnia osoby posiadające odpowiednie kwalifikacje i upoważnienia.

§32

Kontrola, o której mowa w § 31, polega w szczególności na sprawdzeniu:
1) którzy pracownicy mają dostęp do danych osobowych i w jakim zakresie,
2) w jaki sposób użytkownicy zabezpieczają dane osobowe oraz czy stosują określone w niniejszej Polityce środki organizacyjne i techniczne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych,
3) sposobu i zakresu udostępniania danych osobowych innym podmiotom.

§33

1. ASI zobowiązany jest do bieżącego monitorowania systemu zabezpieczeń w systemach informatycznych.

2. W ramach monitorowania należy przeprowadzać w szczególności następujące działania:
   a. okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do odtworzenia danych,
   b. sprawdzanie częstotliwości zmiany haseł przez użytkowników,
   c. kontrolę stosowania innych zabezpieczeń.

§34

1. W celu realizacji powierzonych zadań ADO, IOD i ASI mają prawo w szczególności:
1) kontrolować komórki organizacyjne w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,
2) wydawać polecenia kierownikom komórek organizacyjnych oraz użytkownikom w zakresie bezpieczeństwa danych osobowych,
3) żądać od wszystkich pracowników wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych,
2. Polecenia osób wyznaczonych przez ADO lub IOD do realizacji zadań w zakresie ochrony informacji i bezpieczeństwa systemów informatycznych muszą być bezwzględnie wykonywane przez wszystkich użytkowników.

IX. Przepisy końcowe

§35

Polityka jest dokumentem wewnętrznym i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

§36

Do spraw nieuregulowanych w Polityce stosuje się przepisy ustawy o ochronie danych osobowych i Rozporządzenia.
Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia danych.

PREZES ZARZĄDU
mgr Tomasz Karpiesz