Najbardziej podatnym czynnikiem na powstawanie różnego rodzaju uchybień jest czynnik ludzki

Posted on 2024-11-29

Z Agnieszką Gębicką, dyrektor Biura Ochrony Danych Osobowych w ZUS oraz Sławomirem Wichrowskim, jej zastępcą, rozmawiał Karol Witowski, p.o. Rzecznika Prasowego UODO.

Są Państwo nierozłącznym duetem, który świetnie się uzupełnia. Pani przez lata pełniła funkcję IOD-a w ZUS-ie, zaś Pan był zastępcą IOD. Dziś mam przyjemność pogratulować Wam nowych stanowisk, teraz jesteście dyrekcją nowopowstałego Biura Ochrony Danych Osobowych. Jak ta zmiana w strukturze ZUS wpłynie na pracę zespołu inspektorów ochrony danych w ZUS?

Bardzo dziękujemy! Proces transformacji Naszej komórki w Biuro Ochrony Danych Osobowych następował w drodze naturalnej ewolucji, gdzie stopniowo Zespół wspomagający pracę Inspektora Ochrony Danych dojrzewał do pełnienia jakże ważnej roli w Naszej Instytucji. Dzisiaj możemy powiedzieć z pełną odpowiedzialnością, że jesteśmy otoczeni

grupą fantastycznych, zaangażowanych w swoją pracę osób, na których możemy zawsze liczyć. Jesteśmy zdania, że przeobrażenie się Wieloosobowego Stanowiska Inspektora Ochrony Danych w komórkę rangi departamentu jest namacalną formą uznania Naszych pracowników i docenienia ich ciężkiej pracy. Zmiana rangi komórki ochrony danych osobowych jest też niewątpliwie związana ze skalą realizacji zadań, gdyż jak wiemy Zakład Ubezpieczeń Społecznych jest ogromnym administratorem danych realizującym swe obowiązki na rzecz milionów Klientów. Co do samej organizacji pracy Biura, to należy wspomnieć, że nie odbiega ona co do zasady od tego jak wyglądała ona sprzed wprowadzenia zmian organizacyjnych. Złożoność oraz skala realizowanych zadań powodowała konieczność przekształcenia stosunkowo płaskiej struktury pracowniczej w bardziej zorganizowane instrumenty organizacyjne. Zespoły zadaniowe zostały przekształcone w Wydziały, na czele których stoją naczelnicy oraz powołano wysokospecjalistyczne samodzielne stanowiska, które dopełniają swym zakresem realizowanych zadań czynności wchodzące w zakres Biura Ochrony Danych Osobowych. Wspomniana skala realizacji zadań powoduje, że w swojej strukturze posiadamy wyspecjalizowane wydziały wspomagające Inspektora Ochrony Danych przy realizacji zadań związanych z oceną skutków ochrony danych, doradztwa w zakresie obsługi spraw związanych z naruszeniami przepisów o ochronie danych oraz kwestiami stricte prawnymi oraz związanymi z podnoszeniem kwalifikacji pracowników z zakresu ochrony danych osobowych. Posiadamy również wspominane wcześniej stanowiska odpowiedzialne za realizację audytów zgodności czynności przetwarzania z przepisami o ochronie danych osobowych oraz wspierające pracę Inspektora Ochrony Danych, chociażby przy organizacji coraz częściej realizowanych aktywności edukacyjnych prowadzonych wspólnie z Urzędem Ochrony Danych Osobowych.

Warto również podkreślić, że umiejscowienie Biura Ochrony Danych Osobowych bezpośrednio w Pionie Strategii i Analiz, który podlega Prezesowi ZUS, zapewnia pełną niezależność i autonomię Inspektora Ochrony Danych. Takie usytuowanie organizacyjne jest

Najbardziej podatnym czynnikiem na powstawanie różnego rodzaju uchybień jest czynnik ludzki

nie tylko zgodne z wymaganiami art. 38 RODO dotyczącymi niezależności IOD, ale również wzmacnia jego mandat w zakresie monitorowania zgodności z przepisami o ochronie danych osobowych w tak dużej i złożonej instytucji, jaką jest ZUS. Dzięki tej strukturze IOD ma bezpośredni dostęp do najwyższego kierownictwa, co pozwala na skuteczne raportowanie, podejmowanie kluczowych decyzji oraz natychmiastową reakcję na pojawiające się wyzwania. Jest to także dowód na strategiczne podejście ZUS do ochrony danych osobowych, gdzie IOD nie tylko pełni rolę doradczą, ale także aktywnie uczestniczy w budowaniu systemów ochrony danych, procesów zarządzania ryzykiem oraz działań edukacyjnych i prewencyjnych na rzecz bezpieczeństwa informacji w całej organizacji.

Jak stworzyć prężnie działający zespół? Jaką macie organizację, kulturę pracy i jakie jej elementy są Państwa zdaniem ważne, by praca przynosiła efekty?

Wszystko w naszej opinii zaczyna się od wyboru odpowiednich osób do pracy w komórce ochrony danych osobowych. Problematyka ochrony danych osobowych wymaga ciągłego doskonalenia się, również w obszarach, które z pozoru nie są wprost związane z ochroną praw podstawowych osób fizycznych w związku z przetwarzaniem danych osobowych. To znak naszych czasów oraz kwestia gwałtownego rozwoju techniki. Dlatego też, do pracy w Naszej komórce od zawsze poszukiwaliśmy osób cechujących się nastawieniem na rozwój. Dzisiaj uważamy, że to od nieustannego doskonalenia zależy sukces bądź porażka w tworzeniu zespołu wspomagającego pracę Inspektora Ochrony Danych.

Powyższe powoduje, że pracownicy Biura Ochrony Danych Osobowych często uczestniczą w różnego rodzaju formach podnoszenia kwalifikacji zawodowych, powodujących, że – jak to się potocznie mówi – są „partnerami do rozmowy” we wszelkiego rodzaju dyskusjach problemowych związanych z ochroną danych osobowych. Nierzadko, nasi pracownicy sami wchodzą w role trenerskie, dzieląc się swoją wiedzą i doświadczeniem z pracownikami Naszej Instytucji. Jesteśmy z tego szczególnie dumni. Co do kultury pracy to gdybyśmy musieli opisać jednym słowem jaka jest jej cecha charakterystyczna, to wskazalibyśmy słowo

Najbardziej podatnym czynnikiem na powstawanie różnego rodzaju uchybień jest czynnik ludzki

„otwartość”. Otwartość rozumiana bardzo szeroko i na wielu płaszczyznach, tzn. otwartość na pomysły pracowników, otwartość na pytania z ich strony, czy też otwartość na odmienność zdań. W dzisiejszych czasach poziom wiedzy i świadomości uprawnień wynikających z przepisów prawa wśród społeczeństwa systematycznie rośnie. Z jednej strony jest to powód do zadowolenia, z drugiej zaś powoduje konieczność posiadania zespołów elastycznych, uczących się oraz otwartych na nowe wyzwania, wcześniej nieznanych z uwagi na aktualny poziom techniki lub uregulowania prawne. Dlatego tak ważne jest naszym zdaniem zapewnienie pracownikom poczucia bezpieczeństwa oraz obdarzanie ich zaufaniem. Tylko w taki sposób można mówić nie tylko o efektywnej pracy, ale przede wszystkim pracy, która jest satysfakcjonująca.

W 2022 r. otrzymała Pani tytuł Lidera EMR przyznawany przez firmę PBSG. Wyróżniony został również Zakład Ubezpieczeń Społecznych. Nagroda przyznawana jest osobom oraz organizacjom, które wdrażają najlepsze praktyki w zakresie zarządzania ryzykiem w ochronie danych osobowych.

Tak, wyróżnienie to traktuję jako ogromny zaszczyt zarówno w kategorii osobistej, jak i zawodowej. To namacalna forma uhonorowania Naszych wysiłków jakie były włożone w proces wdrożenia mechanizmów szacowania ryzyka, leżącego u podstaw zarządzania danymi osobowymi. Jako przykład tych działań należy bez wątpienia wskazać wdrożone mechanizmy oceny skutków dla ochrony danych (DPiA), który stanowi obowiązkowy etap prac projektowych realizowanych w Zakładzie Ubezpieczeń Społecznych. Dzisiaj, normą jest, że każdy projekt i inicjatywa realizowana w Zakładzie poprzedzona jest analizą pozwalającą na opisanie całego procesu przetwarzania danych oraz obiektywną ocenę konieczności przetwarzania danych i ich proporcjonalności. Dokonywana analiza w realny sposób pozwala wspomóc zarządzanie ryzykiem naruszenia praw i wolności osób fizycznych.

Rozpowszechnienie praktyki analizy ryzyka w obszarze ochrony danych osobowych w całej organizacji było zadaniem wymagającym konsekwentnego podejścia i wsparcia na wielu

poziomach. Przyzwyczajenie organizacji do konieczności przeprowadzania DPIA dla wszystkich nowych projektów wymagało profesjonalnego i aktywnego wsparcia merytorycznego dla biznesu, jak również dostosowania istniejących wewnętrznych aktów prawnych. Wprowadzono zmiany w procedurach i regulacjach wewnętrznych, aby jasno określić role, obowiązki i harmonogramy związane z procesem DPIA. Dzięki temu DPIA stała się integralnym elementem realizacji projektów, co wpłynęło na budowanie świadomości oraz wzmocnienie odpowiedzialności za ochronę danych na poziomie całej organizacji. W ślad za wdrożeniem opisanych powyżej instytucji normatywnych, implementowano również narzędzie informatyczne, wspomagające przeprowadzania DPiA, o których mowa wyżej, ułatwiając Inspektorowi Ochrony Danych uwzględnianie w swojej pracy ryzyka związanego z operacjami przetwarzania danych osobowych. Wdrożenie tego rodzaju narzędzia wspomagającego stało się niezbędne z punktu widzenia skali Zakładu Ubezpieczeń Społecznych oraz charakteru zadań przez niego wykonywanych.

UODO wraz z ZUS-em zorganizował w tym roku cykl czterech wspólnych spotkań związanych z tematyką ochrony danych osobowych. 9 października br. w Chorzowie podczas seminarium „Czas wyzwań – projektowanie systemów AI oraz wdrożenie NIS2 w organizacji” mówili Państwo nt. wdrożenia tej dyrektywy w organizacji z perspektywy IOD. No właśnie: jak dostosować swoje procesy w organizacjach, by były one zgodne z NIS2? Jakie są Państwa zdaniem najważniejsze podobieństwa i różnice między NIS2 i RODO?

Materia ujęta w dyrektywie NIS 2 jest bardzo szeroka i dotyczy kwestii związanych ze zbudowaniem zdolności w zakresie cyberbezpieczeństwa w całej UE. Powyższe nakłada szereg obowiązków na podmioty kluczowe i ważne, do których zalicza się m.in. Zakład Ubezpieczeń Społecznych. Celem dyrektywy NIS2 jest złagodzenie zagrożeń dla sieci i systemów informatycznych wykorzystywanych do świadczenia usług w najważniejszych sektorach, np. administracji publicznej jak również zapewnienie ciągłości działania w przypadku wystąpienia incydentów. Niezwykle ważną kwestią z punktu widzenia dyrektywy NIS 2 jest zapewnienie przez każdy z podmiotów kluczowych środków zarządzania ryzykiem

Najbardziej podatnym czynnikiem na powstawanie różnego rodzaju uchybień jest czynnik ludzki

w cyberbezpieczeństwie. Środki te obejmują m.in. politykę analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługę incydentów oraz zapewnienie ciągłości działania, np. poprzez zarządzanie kopiami zapasowymi, przywrócenie normalnego działania i zarządzanie kryzysowe.

Podobnie jak RODO, dyrektywa NIS 2 bazuje na podejściu opartym na ryzyku i ciągłym doskonaleniu organizacji na podstawie cyklu PDCA. Obydwie regulacje przewidują dotkliwe kary pieniężne za niedochowanie ich zapisów. Duży nacisk w dyrektywie NIS 2 został położony na systemowe budowanie postaw osób zarządzających i pracowników poprzez organizację cyklicznych szkoleń, mających na celu umiejętność rozpoznawania ryzyk w zakresie cyberbezpieczeństwa oraz zarządzanie nimi. Stanowi to kolejne podobieństwo z RODO, gdzie również przewiduje się powołanie funkcji Inspektora Ochrony Danych, do którego głównych obowiązków należy prowadzenie szkoleń i podejmowanie działań zwiększających świadomość po stronie administratora danych i jego personelu. Dyrektywa NIS 2 podobnie jak RODO implementowana będzie do polskiego porządku prawnego poprzez wprowadzenie przepisów wprowadzających, doszczegóławiając kwestie pozostające w sferze wpływu krajów członkowskich. Podobieństwa między obiema regulacjami obejmują obowiązek zgłaszania – w przypadku NIS 2 są to incydenty związane z cyberbezpieczeństwem, a w przypadku RODO naruszenia ochrony danych osobowych.

Jak powinno wyglądać właściwe wdrożenie polityki AI w organizacji? W czasie seminarium przytoczyła Pani interesujący przykład pracownika, który dla ułatwienia swojej pracy korzysta z Chata GPT i wprowadza do niego informacje prawnie chronione.

Musimy pamiętać, że sztuczna inteligencja to ogromne możliwości i ogromna odpowiedzialność. Te dwie zmienne trzeba obowiązkowo brać pod uwagę przy rozważaniu implementacji sztucznej inteligencji w swojej organizacji. W dzisiejszych czasach widzimy nieustający trend licytowania się różnego rodzaju firm w deklaracjach dotyczących wdrożenia określonych modeli językowych jako integralnych części świadczonych przez

Najbardziej podatnym czynnikiem na powstawanie różnego rodzaju uchybień jest czynnik ludzki

siebie usług.

Na drugiej stronie bieguna widzimy również stosunkowo niewielki procent wdrożeń tej technologii – niewielki w stosunku do skali złożonych deklaracji. To wskazuje jednoznacznie, że implementacja tak zaawansowanej technologii jest wyzwaniem dla organizacji, w tym instytucji sektora finansów publicznych. Wszystkim tym wysiłkom przygląda się europejski ustawodawca, który po raz pierwszy w historii opublikował akt normatywny – AI Act – starający się uporządkować najbardziej palące kwestie związane ze sztuczną inteligencją. Zapisy tego rozporządzenia będą miały bezpośredni wpływ na kierunki wdrożenia sztucznej inteligencji w krajach członkowskich UE. Odpowiadając zatem na pytanie jak powinno wyglądać wdrożenie polityki AI w organizacji należy przede wszystkim wskazać, że powinno ono nastąpić z pełnym poszanowaniem przepisów regulujących tę kwestię. Jest to oczywiście warunek podstawowy, lecz nie jedyne kryterium sukcesu wdrożenia technologii wykorzystującej algorytmy sztucznej inteligencji. Wdrażając regulacje odnoszące się do zasad wykorzystywania sztucznej inteligencji w organizacji należy wskazać, iż regulacje te muszą być „szyte na miarę". Bardzo nęcącym może być chęć skorzystania z wzorców wypracowanych przez inne instytucje, jednakże musimy pamiętać, że organizacja organizacji nie równa, przez co bezrefleksyjne i oderwane od rzeczywistości kopiowanie rozwiązań wypracowanych przez konkurencję może być nie tylko nie najlepszym pomysłem, ale może powodować bardzo konkretne ryzyka. Przykładem może być cytowany na wstępie przypadek wprowadzania do czata GPT informacji chronionych Dlatego też, zaczynając myśleć o wprowadzeniu sztucznej inteligencji oraz norm regulujących jej wykorzystanie musimy zacząć od zidentyfikowania ryzyk jakie są związane z wykorzystywaniem sztucznej inteligencji. Oczywiście, charakter tych ryzyk będzie inny dla firm, a inny dla instytucji publicznych, jednakże niezbędnym jest poznanie ich wszystkich tak, aby im przeciwdziałać.

W pewnych sytuacjach wynik analizy ryzyka może przynieść konstatację, iż przy obecnym stanie techniki nie jesteśmy w stanie implementować mechanizmów sztucznej inteligencji z uwagi na ryzyko, jakiemu nie jesteśmy w stanie przeciwdziałać, narażając tym samym prawa

i wolności osób fizycznych. Kolejnym istotnym elementem, jaki musi być wzięty przy pracach ukierunkowanych na skodyfikowanie zasad wykorzystywania AI w organizacji jest zaangażowanie wszystkich interesariuszy – od Zarządu do pracowników liniowych. Sztuczna inteligencja, niesłusznie zresztą utożsamiana jest wyłącznie z obszarem IT. Obserwujemy jednak, że w coraz większym zakresie to komórki biznesowe są beneficjentami automatyzacji pracy przy wykorzystaniu AI. Dlatego też, zespół odpowiedzialny za wdrożenie sztucznej inteligencji w danej organizacji powinien prowadzić szeroko rozumiane działania informacyjno-edukacyjne wśród wszystkich komórek organizacji, tak aby zmaksymalizować korzyści płynące z jej wdrożenia oraz zminimalizować ewentualne straty nią spowodowane. Osobną kwestią jaka powinna być brana pod uwagę przy procesie wdrożenia sztucznej inteligencji jest analiza spodziewanych korzyści wynikających z jej implementacji w stosunku do poniesionych kosztów związanych z jej wdrożeniem. Kwestia ta jednak w porównaniu do wcześniej poruszonych czynników, tj. analizy ryzyka oraz działań informacyjno-edukacyjnych ma znaczenie drugoplanowe, jednakże obligatoryjnie musi być wzięta pod uwagę, chociażby w jednostkach sektora finansów publicznych.

Bardzo ważnym dla nas wydarzeniem było seminarium UODO i ZUS dot. wdrożenia ustawy o sygnalistach oraz ochrony danych osobowych w miejscu pracy. W swojej prezentacji poruszyli Państwo temat ryzyk naruszenia praw i wolności osób w procesie zgłaszania naruszeń prawa. Jak w praktyce organizacja może zminimalizować wystąpienie tych ryzyk? Jak powinna wyglądać modelowa procedura w tym zakresie?

Sprawami oczywistymi, poruszanymi zresztą podczas naszego wystąpienia były takie czynniki jak maksymalne ograniczenie dostępu do danych sygnalistów oraz zapewnienie odpowiedniego bezpieczeństwa technologicznego – stanowiącego gwarancje anonimowości osób dokonujących zgłoszeń. Równie ważnym czynnikiem jest odpowiedni dobór osób, którym zostaną powierzone obowiązki związane z obsługą spraw sygnalistów. Mówiliśmy również o konieczności przeprowadzania regularnych audytów oraz cyklicznych szkoleniach pracowników z tematyki ochrony danych osobowych. Podnoszone przez nas argumenty nie

straciły w żaden sposób na aktualności.

Dzisiaj jednak wiemy, że najbardziej podatnym czynnikiem na powstawanie różnego rodzaju uchybień jest czynnik ludzki. Dlatego też, w naszych rozważaniach dotyczących najskuteczniejszych metod minimalizujących ryzyko jakie może powstać przy obsłudze tego rodzaju spraw jest kwestia postaw, wiedzy i umiejętności pracowników. W swoje praktyce zawodowej dostrzegamy bowiem niejednoznaczny stosunek pracowników do kwestii dokonywania zgłoszeń przez sygnalistów. Głęboko wierzymy w to, iż ma to swoje podstawy w doświadczeniach historycznych, niemniej jednak konieczna jest zmiana postrzegania w tym zakresie. Musimy przecież pamiętać, że poza powołanymi organami kontroli państwowej oraz wewnętrznymi służbami audytu funkcjonującymi w większości instytucji, czynnik społeczny jest naturalnym dopełnieniem procesu nadzoru. Dlatego też jako podstawowe kryterium powodzenia przy implementacji mechanizmów obsługi spraw sygnalistów wskazalibyśmy kwestię budowania odpowiedniej kultury organizacyjnej. Oczywiście, budowanie tego rodzajów podstaw wśród pracowników jest procesem założonym i czasochłonnym, ale korzyści wynikające z włożonych wysiłków w tym zakresie będą procentować na przyszłość. Stoimy na stanowisku, że wdrożenie przepisów w sprawie ochrony osób zgłaszających naruszenia nie jest kolejnym zadaniem do przysłowiowego „odhaczenia” w drodze jednorazowego wdrożenia, lecz całym procesem, którego powodzenie zależy od pełnego zaangażowania całej organizacji.

Musimy również pamiętać, że natura zgłoszeń dokonywanych przez sygnalistów wymaga szczególnej staranności i delikatności. To od prawidłowej obsługi zgłoszeń, u podstaw których powinna stać ochrona danych osobowych osób dokonujących zgłoszenia, zależy poziom zaufania jakim pracownicy będą obdarzać instytucję zgłoszeń nieprawidłowości jakie pojawiają się w ich miejscu pracy. Przechodząc do procedury, wydaje się zasadnym, aby poza zapisami, które wskazaliśmy jako niezbędne do ujęcia w niej, znalazły się również elementy podkreślające wagę i znaczenie zgłoszeń dokonywanych przez sygnalistów. Bez wątpienia dobrą praktyką będzie zaangażowanie do tworzenia procedury jak najszerszej

Najbardziej podatnym czynnikiem na powstawanie różnego rodzaju uchybień jest czynnik ludzki

grupy interesariuszy, tak aby nie była ona postrzegana jako wyłącznie regulacja dotycząca komórki kontroli wewnętrznej, HR lub innej. Upowszechnienie prac i zaangażowanie do pracy szerokiej grupy pracowników, rekrutujących się z różnych działów jest właśnie elementem budowania wspierającej kultury organizacyjnej.

Mija rok od Waszego wystąpienia w czasie konferencji poświęconej nowym technologiom w kontekście ochrony danych osobowych. Przybliżaliście wtedy problemy audytu IOD z uwagi na wykorzystanie nowych technologii. Temat opisaliście w styczniowym numerze „Biuletynu UODO" (01/2024). Czy do tamtych refleksji możecie coś dodać? Czy pojawiły się jakieś wyzwania, z których rok temu nie zdawaliśmy sobie jeszcze sprawy?

Tematy poruszane w tamtym momencie nie straciły na aktualności, z tą jednak różnicą, że jesteśmy bogatsi o dalsze doświadczenia i co bardzo ważne, pierwszy akt podstawowy regulujący wykorzystanie sztucznej inteligencji przez Państwa członkowskie UE, czyli AI Act. To najlepiej dowodzi, że zidentyfikowane przez nas niebezpieczeństwa związane z wykorzystaniem sztucznej inteligencji w kontekście ochrony danych osobowych są nadal w polu troski i naszej uwagi. Podstawową kwestią, a zarazem najważniejszym niebezpieczeństwem związanym z wykorzystywaniem nowoczesnych technologii, w tym AI jest potencjalne ryzyko dyskryminacji mogące prowadzić do naruszeń praw i wolności osób fizycznych i w konsekwencji do odpowiedzialności podmiotu wykorzystującego tę technologię. Mówiąc o odpowiedzialności mamy na myśli element wzięcia pełnej odpowiedzialności za cały proces przetwarzania danych biorących udział w procesie, począwszy od ich gromadzenia po finalny produkt, jakim jest decyzja firmy ubezpieczeniowej w postaci indywidualizowanej polisy bądź oferty kredytu wygenerowanej przez instytucję finansową.

Te wszystkie nowe technologie wyglądają bardzo atrakcyjnie, ale nie możemy zapominać, że u ich źródła znajdują się – czy też z dużym prawdopodobieństwem mogą się znajdować – nasze dane osobowe. Dzisiejsza praktyka w tym zakresie jest niestety z naszych obserwacji

różna. Przetwarzanie danych osobowych przez wyspecjalizowane podmioty dokonywane jest nierzadko na podstawie zawiłych i nieczytelnych regulaminów z dyskusyjnym prawem konsumenta do wglądu w cały proces. Jeszcze gorzej wygląda sytuacja związana z transparentnością w zakresie miejsc,
w których są wirtualnie przetwarzane dane osobowe.

Dlatego rozpatrując kwestię prawidłowości przetwarzania danych osobowych w kontekście nowych technologii, trzeba mieć na uwadze stały element edukacyjny, uświadamiający wśród społeczeństwa przysługujące prawa oraz zagrożenia wynikające ze stosowania tych technologii. Wydaje się, że tego rodzaju działania uświadamiające powinny odbywać się od najmłodszych lat, przez co zagadnienia związane z ochroną praw osób fizycznych wynikających z przetwarzania danych osobowych przy wykorzystaniu nowoczesnych technologii powinny być stałym elementem programowym w szkołach podstawowych oraz średnich. Jako Biuro Ochrony Danych Osobowych w ZUS widzimy tutaj również swoją rolę oraz możliwość wniesienia realnego wkładu w tego rodzaju działania.

Dziękuję za rozmowę.

Najbardziej podatnym czynnikiem na powstawanie różnego rodzaju uchybień jest czynnik ludzki