AKTUALNOŚCI

Compliance i tajemnica przedsiębiorstwa, czyli na co pracodawcy muszą się przygotować w 2024 roku

Przede wszystkim czeka ich wdrożenie przepisów o sygnalistach, nad którymi znowu ruszyły prace. W dalszej perspektywie muszą mieć na uwadze wdrożenie dyrektywy o jawności wynagrodzeń

Agata Majewska
radca prawny,
Ślązak, Zapiór i Partnerzy

Miniony rok wiązał się z wieloma zmianami ważnymi dla pracodawców. Nie zapowiada się, żeby w 2024 r. tempo zmian miało osłabnąć. Wymuszają je nie tylko nowe regulacje unijne, lecz także rynek, który oczekuje transparentności i konkurencyjności, oraz nowe technologie, które coraz bardziej wpływają na sposób pracy. Kierunek, w którym powinni zmierzać przedsiębiorcy, pokazuje również aktywność organów nadzoru, która w poprzednim roku była dostrzegalna chociażby w działalności prezesa Urzędu Ochrony Danych Osobowych.

Z jakimi wyzwaniami będą się musieli zmierzyć pracodawcy w 2024 r.? Oto wybrane obszary wymagające szczególnej uwagi.

OCHRONA SYGNALISTÓW

17 grudnia 2023 r. minęły dokładnie dwa lata, odkąd w Polsce powinny obowiązywać krajowe przepisy dotyczące zgłaszania naruszeń prawa. Polska jest jednym z dwóch państw członkowskich, które do dziś nie implementowały unijnej dyrektywy. Dotychczas w Sejmie były opracowywane jedynie kolejne wersje projektu ustawy, a ostatnio na stronie Rządowego Centrum Legislacji pojawiła się nowa wersja projektu ustawy o ochronie osób zgłaszających naruszenia prawa.

Świadome swych obowiązków firmy powinny więc przewidująco już teraz przemyśleć i rozpocząć opracowanie polityki wewnętrznych zgłoszeń. Tylko dostosowanie jej do specyfiki danego podmiotu oraz uwzględnienie w niej takich aspektów jak chociażby zgodność z przepisami o ochronie danych osobowych (w tym przez aktualizację wewnętrznych dokumentów i procedur, jak upoważnienia do przetwarzania danych, rejestr czynności przetwarzania, identyfikacja przepływów danych osobowych, dokonanie analizy ryzyka) pozwoli na jej efektywne wdrożenie przy zachowaniu zgodności z innymi przepisami w obszarze compliance.

Dodatkowymi argumentami przemawiającymi za nieodwlekaniem rozwiązań dotyczących zgłaszania naruszeń i ochrony sygnalistów są: z jednej strony krótki – co do zasady miesięczny – okres vacatio legis, jaki przewiduje aktualny projekt ustawy, z drugiej zaś – przewaga konkurencyjna. Zwłaszcza w relacjach z zagranicznymi kontrahentami można dostrzec wzrastającą tendencję do podejmowania współpracy z podmiotami, które mogą się wykazać najwyższym standardem zgodności z europejskimi normami, i to niezależnie od obowiązujących krajowych regulacji.

JAWNOŚĆ WYNAGRODZEŃ

W 2024 r. warto również rozpocząć przygotowania do wprowadzenia rozwiązań związanych implementacją dyrektywy Parlamentu Europejskiego i Rady 2006/54/WE z 5 lipca 2006 r. w sprawie wprowadzenia w życie zasady równości szans oraz równego traktowania kobiet i mężczyzn w dziedzinie zatrudnienia i pracy. Co prawda termin dostosowania polskich przepisów do jej rozwiązań upływa dopiero w 2026 r., jednak w szczególności większe organizacje, w tym te należące do międzynarodowych grup kapitałowych, powinny rozpocząć przegląd siatek wynagrodzeń w poszczególnych grupach pracowników oraz rozpocząć proces ich korygowania, by odpowiadały one zasadom równego wynagrodzenia za pracę taką samą lub takiej samej wartości dla kobiet i mężczyzn. Proces dostosowawczy powinien uwzględniać również taki aspekt jak tajemnica przedsiębiorstwa, która w kontekście jawności wynagrodzeń staje się elementem kluczowym. Nie mniej istotnym elementem będzie odpowiednie uwzględnienie kwestii ochrony danych osobowych (zgodnie z wynikającą z RODO zasadą prywatności w fazie projektowania), w szczególności w zakresie realizacji uprawnień i roszczeń pracowników wynikających z potencjalnych nierówności na płaszczyźnie wynagrodzeń.

SZTUCZNA INTELIGENCJA

W pracy wielu firm, niezależnie od branży, w jakiej działają, coraz częściej jest wykorzystywana sztuczna inteligencja. Z pewnością pozwala to na usprawnienie i automatyzację, jednak z punktu widzenia interesów organizacji (zarówno prawnych, jak i finansowych) kluczowe jest, by odbywało się to w sposób kontrolowany.

Dlatego tak ważne jest wyraźne uregulowanie zasad korzystania z narzędzi AI oraz pogłębianie świadomości pracowników. Może temu służyć w szczególności wewnętrzna polityka korzystania z narzędzi AI, która powinna określać, z jakich rozwiązań i przy zachowaniu jakich zasad bezpieczeństwa (w tym minimalizacji danych) mogą korzystać pracownicy na poszczególnych stanowiskach. Powinna również wprost wskazywać, z jakich narzędzi AI pracownik bezwzględnie nie może korzystać i jakich czynności nie może wykonywać.

Takie działania są ważne chociażby z uwagi na to, że wprowadzane do narzędzi AI dane, w tym te mogące stanowić tajemnicę przedsiębiorstwa oraz dane osobowe, są przetwarzane nie tylko w celu realizacji zleconego programowi zadania, lecz także jego usprawniania (niezależnie od woli użytkownika), czego użytkownicy nie zawsze mają świadomość.

Odpowiednie zabezpieczenie aktywności pracowników i bieżący nadzór nad nią mają również znaczenie w zakresie ochrony prawnoautorskiej powstałych w ten sposób efektów pracy, a także zniwelowania cyberataków.

Dlatego świadoma i dbająca o renomę i bezpieczeństwo finansowe organizacja powinna zwrócić szczególną uwagę na poziom świadomości i umiejętności pracowników używających generatywnej AI oraz wdrożyć, egzekwować i na bieżąco aktualizować w tym obszarze odpowiednie zasady korzystania.

DANE OSOBOWE

Działalność prezesa UODO oraz zagranicznych organów nadzoru daje jasny sygnał, że faktyczne przestrzeganie przepisów o ochronie danych osobowych po ponad pięciu latach obowiązywania RODO jest konieczne i będzie realnie egzekwowane. Staje się to szczególnie ważne w warunkach rozwijającej się sztucznej inteligencji, wzmożonych cyberataków, a także rosnącej świadomości podmiotów danych co do przysługujących im praw.

Jak istotna dla działalności przedsiębiorstwa, w tym jego renomy i pozycji na rynku, jest dbałość o należyte zabezpieczenie i przetwarzanie danych osobowych, mogliśmy się przekonać chociażby na przykładzie ataku na bazę danych Alab Laboratoriów.

Incydent na ogromną skalę związany z ochroną danych, jaki tam nastąpił, może się wiązać z odpowiedzialnością: administracyjną wobec prezesa UODO, odszkodowawczą wobec podmiotu danych, a w określonych przypadkach również karną. Każda z nich to strata wizerunkowa, ale również finansowa dla organizacji. Dodatkowo nieautoryzowany wyciek danych osobowych firmy, stanowiących w danych okolicznościach element jej tajemnicy przedsiębiorstwa, może powodować znaczne straty wizerunkowe i finansowe, osłabiające jej pozycję na rynku.

WAŻNE Wewnętrzna polityka korzystania z narzędzi sztucznej inteligencji powinna określać, z jakich rozwiązań i przy zachowaniu jakich zasad bezpieczeństwa (w tym minimalizacji danych) mogą korzystać pracownicy na poszczególnych stanowiskach.

Nałożone dotychczas przez prezesa UODO kary oraz plany kontroli pokazują, że uwaga administratorów danych powinna koncentrować się w szczególności na zapewnieniu poufności danych i ochronie przed ich ujawnieniem osobom niepowołanym, niezwłocznym notyfikowaniu stwierdzonych naruszeń i odpowiedniej współpracy z organem nadzoru w toku postępowań kontrolnych oraz na stosowaniu odpowiednich – adekwatnych do stwierdzonych ryzyk – zabezpieczeń.

CYBERBEZPIECZEŃSTWO

Wspomniany już najgłośniejszy w ostatnich miesiącach atak hakerski na bazy danych Alab pokazuje, jak istotnym elementem działalności firmy staje się jej bezpieczeństwo cyfrowe, co będzie wymagać także np. szkoleń pracowników. Wyzwaniem, jakie w 2024 r. będzie stać przed organizacjami działającymi w kluczowych dla państwa sektorach, będzie wdrożenie rozwiązań wynikających z tzw. dyrektywy NIS 2, regulującej standardy cyberbezpieczeństwa. Zastąpi ona obecnie obowiązującą dyrektywę NIS. Termin na jej implementację mija 17 października 2024 r. Mimo że obecnie nie toczą się jeszcze prace legislacyjne nad polską ustawą wdrażającą standardy NIS 2, to podmioty mające status średniego i dużego przedsiębiorcy, które należą do kluczowych i ważnych sektorów gospodarki wymienionych w załączniku do dyrektywy, powinny w tym roku rozpocząć proces planowania i wdrażania rozwiązań zapewniających odpowiedni poziom zarządzania ryzykiem w obszarze cyberbezpieczeństwa.

Dyrektywa NIS 2 wprowadza wiele standardów, jakim w zakresie cyberbezpieczeństwa powinny odpowiadać podmioty należące do wybranych branż. Dostosowanie się do nich będzie wymagać rozwiązań zarówno organizacyjnych (jak polityka analizy ryzyka i bezpieczeństwa systemów informatycznych, ocena skuteczności środków zarządzania ryzykiem, opracowanie zasad obsługi incydentów cyberbezpieczeństwa, szkolenia), jak i informatycznych (m.in. wdrożenie odpowiednich środków technicznych w celu zabezpieczenia systemów informatycznych, regularne audyty wykrywające potencjalne zagrożenia). Dodatkowo konieczne będzie informowanie właściwego organu o poważnych incydentach. Przepisy będą rozszerzać krąg podmiotów oraz zakres obowiązków wynikających z dotychczasowej ustawy o cyberbezpieczeństwie. Wynika to przede wszystkim z rosnącego systematycznie ryzyka zagrożeń cyberatakami, które mogą stanowić zagrożenie nie tylko dla samych dotkniętych nimi przedsiębiorców, lecz także dla dostępności kluczowych dla społeczeństwa usług.

RAPORTOWANIE NIEFINANSOWE

Raportowanie niefinansowe to nowy standard wyznaczony przez dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2464 z 14 grudnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 537/2014, dyrektywy 2004/109/WE, dyrektywy 2006/43/WE oraz dyrektywy 2013/34/UE w odniesieniu do sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju. Obejmuje ono trzy główne obszary: środowisko, społeczeństwo i ład korporacyjny (ang. Environmental, Society, Governance – w skrócie ESG). W kontekście pracodawców ważne będzie zatem wykazywanie np. podjęcia działań dotyczących przeciwdziałania mobbingowi oraz zapewnienia równości wynagrodzeń.

Dyrektywa powinna zostać wdrożona w Polsce do 6 lipca 2024 r. Pierwsze sprawozdania dotyczące roku obrotowego rozpoczynającego się od 1 stycznia 2024 r. będą miały obowiązek złożyć podmioty podlegające dyrektywie Parlamentu Europejskiego i Rady 2014/95/UE z 22 października 2014 r. zmieniającej dyrektywę 2013/34/UE w odniesieniu do ujawniania informacji niefinansowych i informacji dotyczących różnorodności przez niektóre duże jednostki oraz grupy.

Celem sprawozdań ESG jest zapewnienie spójnego i porównywalnego między poszczególnymi podmiotami dostępu do informacji o zrównoważonym rozwoju. Ma to służyć m.in. odpowiedniej wycenie spółek przez inwestorów, ograniczeniu praktyk washingowych, poprawie wizerunku firm wobec konsumentów. Mimo że obowiązek raportowania będzie dotyczyć w początkowych etapach wyłącznie największych podmiotów (m.in. notowanych na giełdzie oraz osiągających odpowiedni pułap przychodów lub sumy bilansowej), to stopniowo przestaje on być już jedynie dobrowolnym rynkowym trendem. Nawet podmioty, które formalnie nie są jeszcze (lub nie będą w ogóle) obowiązane do raportowania w zakresie ESG, powinny się pochylić nad tym obszarem, jeśli zamierzają utrzymać wysoką konkurencyjność na rynku i zyskać zaufanie klientów i inwestorów. ©℗

Podstawa prawna

- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE z 2016 r. L 119, s. 1; RODO)
- dyrektywa Parlamentu Europejskiego i Rady 2006/54/WE z 5 lipca 2006 r. w sprawie wprowadzenia w życie zasady równości szans oraz równego traktowania kobiet i mężczyzn w dziedzinie zatrudnienia i pracy (Dz.Urz. UE z 2006 r. L 204, s. 23)
- dyrektywa PE i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148; Dz.Urz. UE z 2022 r. L 333, s. 80; dyrektywa NIS 2)
- dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2464 z 14 grudnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 537/2014, dyrektywy 2004/109/WE, dyrektywy 2006/43/WE oraz dyrektywy 2013/34/UE w odniesieniu do sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju (Dz.Urz. UE z 2022 r. L 322, s. 15)
- dyrektywa Parlamentu Europejskiego i Rady 2014/95/UE z 22 października 2014 r. zmieniająca dyrektywę 2013/34/UE w odniesieniu do ujawniania informacji niefinansowych i informacji dotyczących różnorodności przez niektóre duże jednostki oraz grupy (Dz.Urz. UE z 2014 r. L 330, s. 1)