

Jak przeżyć okres świąteczny i nie zwariować? Zastanawiamy się nad ciągłością działania

W TYM WYDANIU:

Modele rekrutacji a ochrona danych osobowych: przewodnik praktyczny

2

Znaczenie zarządzania ciągłością działania w prowadzeniu biznesu w oparciu o wymagania normy ISO 22301

9

Prasówka

13

Kary z Polski i świata

17



Agata Strzyżewska

Modele rekrutacji a ochrona danych osobowych: przewodnik praktyczny

Nie ulega wątpliwości, że proces rekrutacji oraz Ogólne Rozporządzenie o Ochronie Danych Osobowych są ze sobą bardzo ściśle powiązane. Rekrutacja zawsze będzie wiązała się z przetwarzaniem danych osobowych kandydatów do pracy. CV, listy motywacyjne, rekomendacje to tylko niektóre z dokumentów aplikacyjnych, z których w procesie rekrutacji zbierane są dane osobowe.

W niniejszym artykule pochylimy się nad procesem rekrutacji, w ujęciu praktycznym z punktu widzenia pracodawcy oraz innych osób zaangażowanych w proces, a także zestawimy podejście różnych instytucji systemu prawnego do kluczowych aspektów związanych z rekrutacją, także w kontekście wymogów prawa.

Modele rekrutacji, czyli kto jest kim w najczęściej spotykanych modelach rekrutacji

Właściwe określenie roli administratora danych w procesie rekrutacji jest pierwszym krokiem do legalnego przeprowadzenia procesu rekrutacji. Zgodnie z art. 4 punkt 7 RODO, administrator to osoba lub instytucja, która decyduje o celach i sposobach przetwarzania danych osobowych. W kontekście rekrutacji może to być zarówno pracodawca, jak i zewnętrzna firma rekrutacyjna.

W obecnych czasach najczęściej spotykamy się z modelami rekrutacji, o których poniżej.

REKRUTACJA ZWYKŁA

Jest to wciąż jeden z najbardziej popularnych modeli rekrutacji. Proces rekrutacji zarządzany jest wewnętrznie przez pracodawcę i jego zespół – najczęściej wykorzystując własną stronę www, gdzie zamieszczane są ogłoszenia o poszukiwaniu osób na konkretne stanowisko pracy. Nie pozostawia wątpliwości, że w tym modelu to właśnie **pracodawca jest administratorem danych osobowych**. Warto wspomnieć, że w tym przypadku zewnętrzny **dostawca usług**, któremu administrator powierzył zaprojektowanie i hosting swojej strony internetowej, a także stworzenie dedykowanej przestrzeni do rekrutacji, takiej jak formularz umożliwiający przesłanie CV i listu motywacyjnego, **może zostać zakwalifikowany jako podmiot przetwarzający dane**.

REKRUTACJA PRZY POMOCY DOSTAWCY USŁUG ONLINE

W dzisiejszym bardzo szybko rozwijającym się cyfrowo świecie w zasadzie na porządku dziennym jest ten model rekrutacji, w którym to pracodawca wykorzystuje platformy internetowe specjalizujące się w poszukiwaniu talentów. Także w przypadku tego modelu rekrutacji **pracodawca jest**

administratorem danych osobowych, ponieważ to on inicjuje rekrutację, w ramach której określa cel i zakres przetwarzania danych. W tym przypadku **dostawca usług internetowych działa jako podmiot przetwarzający** dane w imieniu pracodawcy.

REKRUTACJA Z POLECENIA, CZYLI ZYSKUJĄCE NA POPULARNOŚCI PROGRAMY POLECEŃ PRACOWNICZYCH

Przypomnijmy, że w tym modelu rekrutacji do pracodawcy trafia kandydatura osoby poleconej przez obecnego pracownika. W rekrutacji uczestniczą trzy strony: **pracodawca jako administrator danych osobowych**, obecny pracownik oraz osoba polecana.

W tym miejscu warto pochylić się nad sposobem, w jaki kandydatura ta powinna trafić na ręce pracodawcy, aby zapewnić pełną zgodność z RODO. Najbezpieczniejszym rozwiązaniem, w stosunku do wymagań, jakie są stawiane przez RODO, będzie stworzenie przestrzeni do przekazania CV bezpośrednio przez osobę poleconą. W tym modelu rekomenduje się, aby zakres danych, które pracodawcy przekazuje obecny pracownik, był możliwie jak najwęższy i ograniczał się tylko do danych identyfikacyjnych w zakresie imienia, nazwiska i np. adresu e-mail.

W praktyce oznacza to, że osoba polecona dokona samodzielnego przekazania przy pomocy np. linka do oferty pracy przesłanego przez pracownika mailem czy komunikatorem internetowym.

Wówczas jako pracodawca będziemy w stanie dopełnić ciężących na nas obowiązków. Damy osobie poleconej możliwość zapoznania się z klauzulą informacyjną oraz wyrażenia zgody na przekazanie przez obecnego pracownika danych umożliwiających identyfikację kandydatury poprzez powiązanie jej z danymi osoby. Przy zastosowaniu takiego rozwiązania nie będzie wątpliwości czy udzielona zgoda jest jednoznaczna, czy dobrowolna, jak mogłoby to mieć miejsce w przypadku pozyskania zgody osoby poleconej przez obecnego pracownika.

AGENCJA PRACY TYMCZASOWEJ

Pomimo tego, że korzystanie z usług agencji pracy tymczasowej jest stosowanym od dawna modelem rekrutacji, po wejściu w życie RODO sprawy skomplikowała kwestia po czyjej stronie pracodawcy, użytkownika czy agencji pracy tymczasowej leży

administrowanie danymi kandydatów do pracy.

Nie ma wątpliwości co do określenia roli, jaką w procesie pełni agencja pracy tymczasowej, która zarówno na etapie rekrutacji, jak i zatrudniania pracowników tymczasowych jest administratorem danych osobowych, mając za cel identyfikację odpowiednich kandydatów na dane stanowisko pracy oraz zarządzanie całym procesem rekrutacyjnym. Staje się również pracodawcą w myśl definicji zawartej w Kodeksie Pracy.

Sytuacja nie jest już tak klarowna w przypadku pracodawcy użytkownika, a to za sprawą dwóch odmiennych interpretacji roli, jaką w procesie pełni pracodawca użytkownik. Jak wskazuje Urząd Ochrony Danych Osobowych w opublikowanym poradniku dla pracodawców, agencja pracy tymczasowej (w kontekście Ustawy z dnia 9 lipca 2003 o zatrudnianiu pracowników tymczasowych) powinna zawrzeć z pracodawcą użytkownikiem stosowną umowę powierzenia przetwarzania danych. Umowa ta powinna precyzyjnie określać zakres i cel przetwarzania danych przez pracodawcę użytkownika, nadając mu tym samym status podmiotu przetwarzającego.

Jednocześnie UODO stwierdza, że na pracodawcy użytkownika ciążyą także pewne obowiązki pracodawcy, wymienione we wspomnianej powyżej Ustawie, takie jak np. prowadzenie ewidencji czasu pracy. Te obowiązki sprawiają, że pracodawca użytkownik w pewnych aspektach uzyskuje status administratora danych osobowych.

Nie wszyscy jednak zgadzają się z podejściem UODO, wskazującym na podwójną rolę pracodawcy użytkownika. Część środowiska zajmującego się ochroną danych osobowych wskazuje, jednakże, że agencję pracy tymczasowej z pracodawcą użytkownikiem łączy wyłączenie relacja ADO-ADO, bowiem agencja pracy tymczasowej udostępnia dane pracowników, takie jak imię i nazwisko, innemu podmiotowi, czyni to w celu umożliwienia temu podmiotowi realizacji własnych zadań przetwarzania danych (na przykład prowadzenia ewidencji czasu pracy). W tej sytuacji podmiot otrzymujący dane osobowe pracowników nie przetwarza ich w imieniu agencji jako administratora, lecz realizuje własne cele przetwarzania.

W naszej opinii współpraca w relacji agencja pracy tymczasowej, a pracodawca to standardowy model

udostępniania danych: pracodawcy użytkownikowi przez agencję. Pracodawca korzystający z usług agencji pracy tymczasowej do pozyskiwania pracowników działa w realizacji własnych celów, co czyni go niezależnym i odrębnym administratorem danych osobowych. Co za tym idzie, w tym modelu rekrutacji obecni są dwaj niezależni administratorzy danych: agencja pracy tymczasowej oraz pracodawca użytkownik.

W związku z tym, regulacje dotyczące udostępnienia danych osobowych powinny być szczegółowo określone w umowie głównej lub ramowej, która łączy zakład pracy z agencją pracy tymczasowej. Postanowienia te powinny zawierać odpowiednią klauzulę poufności, aby zapewnić ochronę tych danych.

AGENCJA HEADHUNTERSKA

W przypadku korzystania przez pracodawcę z usług agencji headhunterskiej sprawa określenia roli, jaką pełnią strony wydaje się być mniej skomplikowana. W tym scenariuszu klient, czyli potencjalny pracodawca, jest administratorem danych osobowych kandydatów. To on określa cele i sposoby przetwarzania tych danych, mając pełną

decyzyjność podczas całego procesu. W związku z tym konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych między klientem a agencją rekrutacyjną. W ramach tej umowy klient powierza agencji przetwarzanie danych osób ubiegających się o pracę.

Drugi scenariusz, gdy agencja rekrutacyjna korzysta ze swoich własnych baz danych osobowych kandydatów lub samodzielnie ich poszukuje (np. przez publikowanie ogłoszeń o pracę, kontaktowanie się z kandydatami poprzez dedykowane portale). Włącza ona dane osobowe kandydatów do swoich zbiorów danych.

W takim przypadku agencja rekrutacyjna działa jako administrator danych osobowych kandydatów, ponieważ to ona decyduje o celach i sposobach ich przetwarzania. Agencja ma obowiązek wypełnić wymogi informacyjne określone w RODO, ponieważ przetwarza dane w swoim własnym celu, którym jest przeprowadzenie pierwszego etapu rekrutacji, czyli pozyskanie CV i selekcjonowanie kandydatów. Agencja przetwarza dane osób poszukujących pracy nie tylko na potrzeby konkretnej rekrutacji, ale również w celu przyszłych procesów rekrutacyjnych

LexDigital

	REKRUTACJA ZWYKŁA	REKRUTACJA PRZY POMOCY DOSTAWCY USŁUG ONLINE	REKRUTACJA Z POLECENIA	REKRUTACJA PRZY POMOCY APT (WG. UODO)	REKRUTACJA PRZY POMOCY APT (PRAKTYCY)	REKRUTACJA PRZY POMOCY AGENCJI HEADHUNTERSKIEJ (MODEL 1)	REKRUTACJA PRZY POMOCY AGENCJI HEADHUNTERSKIEJ (MODEL 2)
PRACODAWCA JAKO ADMINISTRATOR	✓	✓	✓	✓	✓	✓	✓
PRACODAWCA JAKO PODMIOT PRZETWARZAJĄCY				✓			
ZEWNĘTRZNY DOSTAWCA USŁUG INTERNETOWYCH JAKO PODMIOT PRZETWARZAJĄCY		✓					
AGENCJA PRACY TYMCZASOWEJ JAKO ADMINISTRATOR				✓	✓		
AGENCJA HEADHUNTERSKA JAKO PODMIOT PRZETWARZAJĄCY						✓	
AGENCJA HEADHUNTERSKA JAKO ADMINISTRATOR							✓

dla różnych klientów.

Agencja rekrutacyjna wyszukuje w swoich bazach danych kandydatów, spełniających wymagania określone w umowie o współpracę. Gdy udostępnia dane osobowe (CV, list motywacyjny) potencjalnego pracownika klientowi, który zlecił rekrutację, klient ten w momencie otrzymania dokumentów aplikacyjnych staje się administratorem danych osobowych. Na nim ciąży wtórny obowiązek informacyjny wynikający z art. 14 RODO.

Retencja danych kandydatów do pracy

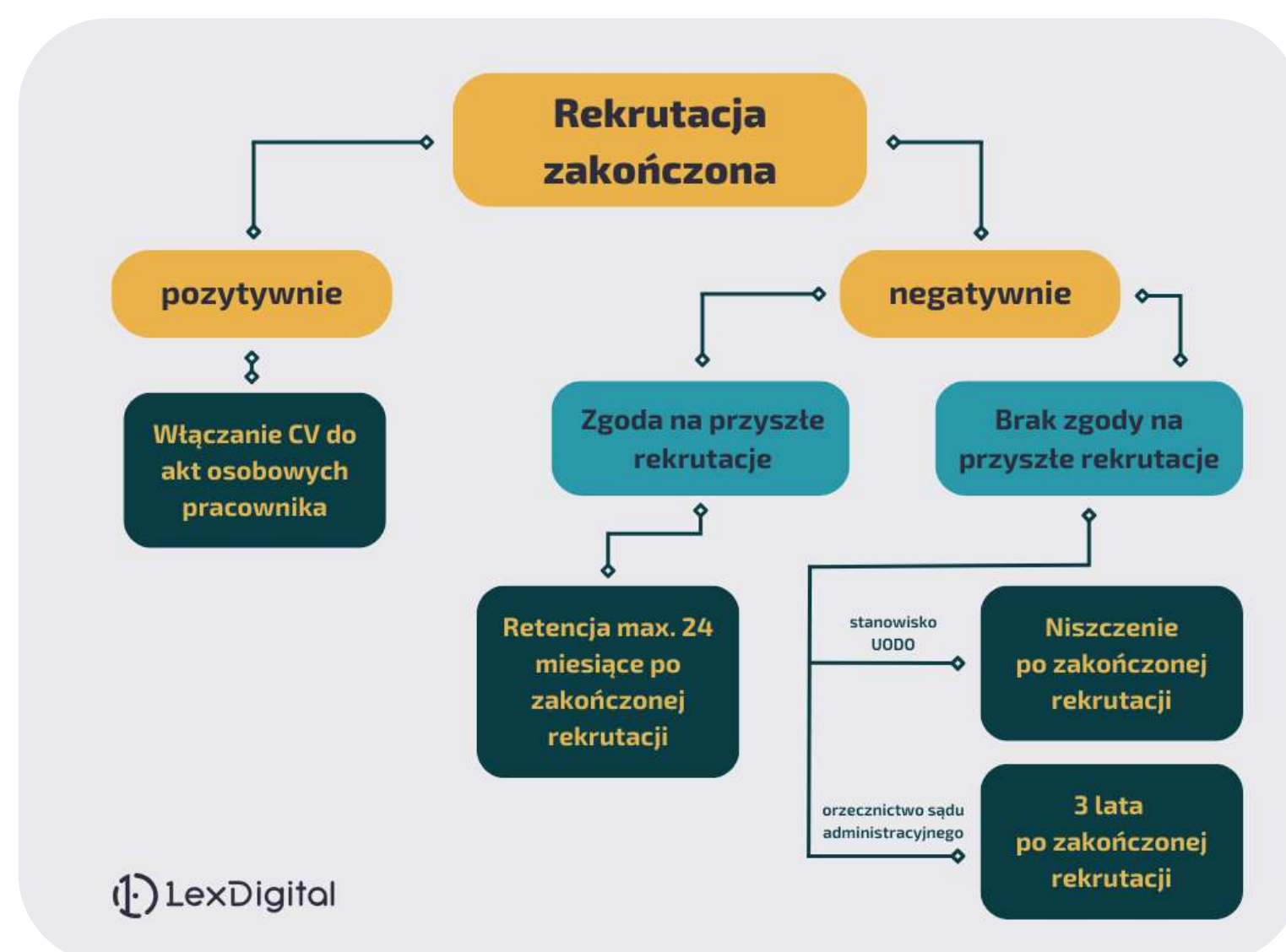
Niezależnie od modelu rekrutacji, w którym pozyskujemy dane kandydatów, osoby prowadzące proces rekrutacji wciąż zadają sobie pytanie, przez jaki okres mogą przechowywać dane kandydatów. Trzeba przyznać, że jest to nie lada temat do rozważań, ponieważ z jednej strony mamy jasne wytyczne UODO, z drugiej decyzje administracyjne sądów i wytyczne innych organów nadzorczych. Ale od początku.

Przy ustaleniu okresu retencji fundamentalne znaczenie będzie miało, czy kandydat wyraził zgodę na przyszłe rekrutacje, czy też nie.

Zacznijmy od sytuacji, gdy kandydat do pracy nie wyraził zgody na udział w przyszłych procesach rekrutacji, czy też jako pracodawca przeprowadzamy jednorazowy proces rekrutacji. Zgodnie z oficjalnym stanowiskiem UODO w takiej sytuacji pracodawca powinien w kolejności: zgromadzić CV -> przeprowadzić selekcję -> dokonać wyboru odpowiedniego kandydata lub kandydatki -> a następnie usunąć pozostałe zgromadzone CV. UODO jednoznacznie wskazuje, że niedopuszczalne jest przetwarzanie danych osobowych jedynie w celu zabezpieczenia się przed potencjalnymi roszczeniami ze strony osoby, której dane dotyczą. Urząd Ochrony Danych Osobowych argumentuje powyższe stwierdzenie, że postępowanie w ten sposób, mogłoby prowadzić do wątpliwości dotyczących tego, jak długo należy przechowywać dane osobowe, szczególnie w sytuacji, gdy dana osoba nie zdecyduje się na podjęcie kroków prawnych przeciwko pracodawcy.

Cały przebieg tej sytuacji nieco inaczej widzi Wojewódzki Sąd Administracyjny w Warszawie, który

to wyrokiem z dnia 4 sierpnia 2022 roku (II SA/Wa 542/22), uchylił decyzję Prezesa UODO. W decyzji tej organ nadzorczy udzielił pracodawcy upomnienia za, według jego oceny, nieuzasadnione przetwarzanie danych osobowych kandydatki do pracy po zakończeniu procesu rekrutacji. W ocenie Sądu CV powinno być przechowywane przez określony czas ze względu na wymogi Kodeksu pracy, które mają na celu zapobieganie dyskryminacji. Zgodnie z brzmieniem artykułu 183d Kodeksu pracy, osoba, w stosunku do której pracodawca naruszył zasadę równego traktowania w zatrudnieniu (w tym także kandydat ubiegający się o zatrudnienie), ma prawo do żądania odszkodowania. Co więcej, przepisy prawa pracy wskazują nawet konkretny 3-letni termin przedawnienia tego roszczenia. Idąc drogą orzecznictwa Sądu, CV należy usuwać po upływie 3 lat od zakończenia procesu rekrutacji.



Niestety jest to typowy przypadek, w którym dochodzi do konfliktu między różnymi istotnymi normami prawnymi. Pracodawca jako administrator danych niezależnie od podjętej decyzji ponosi ryzyko, że nie będzie ona zgodna z wymaganiami jednej ze stron.

Przejdźmy teraz do sytuacji, w której kandydat wyraził zgodę na udział w przyszłych procesach rekrutacji. Prawdą jest, że w także w tym przypadku RODO nie oferuje nam gotowej odpowiedzi. Nie określa konkretnych terminów przechowywania danych kandydatów do pracy, w tym tych, którzy wyrazili zgodę na uczestnictwo w przyszłych rekrutacjach. Jednakże rozporządzenie zwraca uwagę na dwie kluczowe zasady: minimalizacji danych (gromadzenie i przechowywanie tylko tych danych, które są niezbędne, np. do celów rekrutacyjnych) oraz

ograniczenia czasowego przetwarzania danych (jeśli dane stają się zbędne, powinny być usunięte lub zanonimizowane).

Odpowiedzialność za ustalenie okresu przechowywania danych spoczywa na pracodawcy, który powinien wziąć pod uwagę m.in. własne potrzeby związane z charakterem prowadzonych rekrutacji oraz czasem, przez który dane kandydata pozostają aktualne i przydatne dla celów przyszłych rekrutacji. Jako najczęściej stosowaną praktykę wskazuje się okres 12 lub 24 miesięcy. Francuski organ nadzorczy w opublikowanym Przewodniku dot. rekrutacji wskazuje, że „W tym konkretnym celu, jakim jest zasilenie „puli kandydatów” w tym kontekście, zaleca się, aby okres przechowywania danych był rozsądny, w zależności od rodzaju danego stanowiska, a w każdym razie zasadniczo nie przekraczał dwóch lat od ostatniego kontaktu z daną osobą”.

Jak wygląda sytuacja z danymi kandydata, dla którego proces rekrutacji zakończył się sukcesem?

Po pomyślnym zakończeniu procesu rekrutacji, dokumenty takie jak CV i list motywacyjny są włączane do części A akt osobowych pracownika. Informacje zawarte w tych dokumentach nie mogą już być wykorzystywane w innym celu. W przypadku osób zatrudnionych przed 1 stycznia 2019 roku okres przechowywania akt osobowych wynosi 50 lat. Osoby zatrudnione po 1 stycznia 2019 roku, ich akta są przechowywane przez 10 lat.

Dane niezbędne do zawarcia umowy o pracę, częściowo pokrywające się z danymi kandydata, muszą zostać zebrane na nowo w związku z nowym celem, jakim jest zawarcie umowy, zazwyczaj poprzez wypełnienie kwestionariusza osobowego.



Jakie sytuacje w całym procesie rekrutacyjnym wymagają bezwzględnego pozyskania wyraźnej i świadomej zgody?

Kiedy zgoda odbierana jest jako oświadczenie woli czy świadome działanie, a w jakich przypadkach nawet zgoda kandydata do pracy nie daje pracodawcy podstawy do przetwarzania pozyskanych danych?

Zgody w procesie rekrutacji to chyba jeden z najszerzej opisywanych i interpretowanych obszarów na gruncie przenikania się przepisów o ochronie danych osobowych z rekrutacją.

Wokół procesu odbierania zgód narosło wiele mitów, a rekruterzy przez długi czas nie radzili sobie z mechanizmami zarządzania zgodami i na wszelki wypadek odbierali je niemal na wszystko.

Na szczęście po przeszło 5 latach, odkąd rozpoczęliśmy stosowanie RODO, posiadamy rekomendacje oraz interpretacje, które jasno wskazują zasadność odbierania zgody kandydata do pracy.

1. Zgoda na przetwarzanie danych osobowych w ramach przeprowadzanego procesu rekrutacji

Można z całym przekonaniem powiedzieć, że taka zgoda nie istnieje. W procesie rekrutacji to nie zgoda stanowi podstawę prawną przetwarzania danych. Dane w zakresie wskazanym w art. 22¹ § 1 ustawy z dnia 26 czerwca 1974 r. Kodeksu pracy, przetwarzane są w oparciu o art. 6 ust. 1 lit. b) RODO tj. podejmowanie niezbędnych działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.

2. Zgoda na przetwarzanie danych wykraczających poza zakres wskazany w art. 22¹ § 1 ustawy z dnia 26 czerwca 1974 r. Kodeksu pracy

W tej sytuacji za podstawę prawną przetwarzania tych danych należy wskazać zgodę. Jednakże jest to zgoda, która wynika ze świadomego działania kandydata do pracy, w momencie przekazania tych

danych pracodawcy w CV czy za pomocą formularza zgłoszeniowego.

3. Zgoda na przetwarzanie danych szczególnych kategorii.

Może się zdarzyć sytuacja, w której poza zakresem danych wskazanych w art. 22¹ § 1 ustawy z dnia 26 czerwca 1974 r. Kodeksu pracy, a nawet danych zwykłych wykraczających poza ten zakres w CV kandydata pojawią się dane szczególnych kategorii np. dane dotyczące np. stanu zdrowia. Zgodnie z brzmieniem art. 22(1)(b) § 1 Kodeksu Pracy, tzw. dane wrażliwe (dane szczególnej kategorii) mogą być przetwarzane przez pracodawcę jedynie, jeśli ich przekazanie następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika. Jest to ważne, ponieważ pracodawca nie może wymagać, ani zachęcać kandydatów do przekazywania takich danych w swojej aplikacji.

W przypadku, gdy kandydat z własnej inicjatywy przekazuje dane wrażliwe, takie jak informacje o stanie zdrowia, powinien wyrazić odrębną zgodę na ich przetwarzanie. Wyjątek stanowi sytuacja, gdy przetwarzanie takich danych jest dozwolone lub wymagane na podstawie innych przepisów prawa, na przykład przy zatrudnianiu osób z niepełnosprawnościami.

4. Zgoda na udział w przyszłych procesach rekrutacyjnych.

Aby pracodawca mógł rozpatrywać kandydaturę w ramach przyszłych procesów rekrutacyjnych, musi uzyskać od kandydata odrębną wyraźną zgodę. Najczęściej zgoda ta przyjmuje formę klauzuli w CV lub klauzuli w formie checkboxa. Zależać to będzie wyłącznie od samej formy przeprowadzania rekrutacji i mechanizmu przekazywania CV pracodawcy.

Nawet za zgodą pracodawca nie ma prawa żądać przedłożenia:

5. Danych o wyrokach skazujących

W tym przypadku, nawet jeśli kandydat do pracy wyraziłby zgodę, pracodawca nie może przetwarzać danych dotyczących wyroków skazujących, czynów zabronionych czy powiązanych środków bezpieczeństwa. Podstawą przetwarzania tego rodzaju danych musi być wyraźny przepis prawa. W praktyce oznacza to, że pracodawca może przetwarzać takie dane, jedynie w celu

przeprowadzenia weryfikacji w ramach procesu rekrutacyjnego na stanowiska wymagające sprawdzenia przeszłości kandydata. Stanowiska te związane są m.in z bezpieczeństwem publicznym, pracą z dziećmi, czy wymagające wysokiego stopnia zaufania.

PRZEBIEG ROZMOWY KWALIFIKACYJNEJ – o co może pytać pracodawca, a jakich czynności bezwzględnie nie może się podejmować

Przyjrzymy się teraz, jak powinien przebiegać ostatni etap procesu rekrutacyjnego, czyli rozmowa rekrutacyjna, tak aby pracodawcy nie można było zarzucić działań niezgodnych z RODO.

Fundamentalną zasadą, zgodnie z art. 221 Kodeksu pracy, wskazuje, że w trakcie rozmowy kwalifikacyjnej dopuszczalne jest pytanie kandydata tylko o te dane, które są wymienione w tym artykule. Sam kandydat nie jest ograniczony tym przepisem i może dobrowolnie podzielić się dodatkowymi informacjami.

Pracodawca nie powinien robić notatek z rozmowy rekrutacyjnej bezpośrednio na kopiach dokumentów kandydata, które mogą być później przechowywane w aktach osobowych. Jeśli kandydat zostanie oceniony negatywnie, wszelkie notatki z tej oceny powinny być przechowywane tylko do czasu zakończenia procesu rekrutacji, aby uniknąć tworzenia tzw. czarnych list kandydatów. Notatki powinny odnosić się jedynie do kwalifikacji pracownika, a nie powinny go dyskryminować.

Pracodawca może skontaktować się z poprzednim pracodawcą kandydata wyłącznie w przypadku, gdy otrzyma od kandydata referencje zawierające zgodę na taki kontakt. Weryfikacja referencji bez zgody kandydata jest niedopuszczalna.

Ważne! Jeśli uzyskujemy od kandydata dane kontaktowe osoby reprezentującej jego poprzedniego pracodawcę, nie jest wymagana zgoda tej osoby na kontakt. Jednakże jesteśmy zobowiązani spełnić wobec tej osoby obowiązek informacyjny.

W świetle polskiego prawa niedopuszczalne jest potwierdzanie autentyczności dyplomów ukończenia studiów wyższych oraz innych danych dostarczonych przez kandydata w procesie rekrutacji poprzez kontaktowanie się z instytucjami, które wydały te dokumenty. Przepisy krajowe generalnie nie przyznają pracodawcy prawa do weryfikacji prawdziwości dokumentów i danych w nich zawartych, które zostały przedłożone przez kandydatów w trakcie rekrutacji.

Jak wskazuje poradnik Urzędu Ochrony Danych Osobowych, pracodawca może korzystać z informacji zawartych na portalu LinkedIn w celu potwierdzenia historii zatrudnienia kandydata. Jest to dopuszczalne ze względu na charakter portalu LinkedIn, który ma na celu udostępnianie informacji o historii zatrudnienia i doświadczeniu zawodowym. Jednakże pozyskiwanie danych osobowych kandydatów do pracy z innych portali społecznościowych, takich jak na przykład Facebook, nie jest uznawane za dopuszczalne, ponieważ te platformy służą innym celom i nie są przeznaczone do dzielenia się

informacjami zawodowymi.

Podsumowanie

Podsumowując, proces rekrutacji w świetle RODO wymaga od pracodawców i innych uczestników rekrutacji, w tym agencji rekrutacyjnych zwracania szczególnej uwagi na zarządzanie danymi osobowymi. Istotne jest właściwe określenie roli administratora danych oraz zastosowanie się do zasad minimalizacji i ograniczenia czasowego przetwarzania danych. Pracodawcy muszą także zapewnić zgodność praktyk rekrutacyjnych, w tym rozmów kwalifikacyjnych, z przepisami o ochronie danych, aby uniknąć naruszeń i potencjalnych sankcji.

W dobie cyfryzacji i rosnącej świadomości prawnej kandydatów, zrozumienie i przestrzeganie RODO staje się nie tylko obowiązkiem, ale i elementem budowania zaufania i profesjonalnego wizerunku na rynku pracy.



5 PROSTYCH KROKÓW NA DRODZE REKRUTACJI, ZGODNEJ Z RODO

- **Zawsze pytaj i dokumentuj zgodę kandydata**
- **Ciągle doskonal swoją politykę prywatności w zakresie rekrutacji**
- **Zachowaj przejrzystość wobec kandydatów w ciągu całej rekrutacji**
- **Regularnie przeprowadzaj audyt danych**
- **Korzystaj z systemu śledzenia kandydatów zgodnego z RODO**



Dariusz Janiak

Znaczenie zarządzania ciągłością działania w prowadzeniu biznesu w oparciu o wymagania normy ISO 22301

1. Sytuacje kryzysowe w działalności biznesowej.

To nie rzadki przypadek, kiedy firma uświadamia sobie wagę zapewnienia ciągłości działania dopiero w chwili spotykającej ją sytuacji kryzysowej. Na skutek takich zdarzeń jak pandemia, katastrofa budowlana, klęski żywiołowe, atak hakerski i inne, firma nagle doświadcza poważnych przeszkód w bieżącym funkcjonowaniu, czego wyrazem może być np. niedostępność personelu, utrata lokalizacji, w której prowadzona jest działalność firmy, zniszczenie ważnych aktywów w postaci sprzętu, infrastruktury, surowców, produktów, brak możliwości dostępu do krytycznych informacji, baz danych lub innych zasobów firmy. Mimo iż takie sytuacje są do przewidzenia, firmy nie zawsze mają wypracowane skuteczne sposoby postępowania, by działać zarówno przed, jak i po wystąpieniu kryzysu. Czas niedostępności kluczowych procesów upływa, a wraz z nim odpływają klienci, topnieją zamówienia, piętrzą się reklamacje, zalegają towary, psują się produkty. O firmie zaczyna być głośno, ale w tym złym tego słowa znaczeniu. Im dłuższy przestój organizacji tym większa frustracja klientów, partnerów i kontrahentów. Pojawia się groźba kar umownych, reklamacji i widmo zapłaty odszkodowań.

2. Ciągłość działania.

Pierwszy etap kryzysu najczęściej cechuje się znaczną dynamiką. Stosowane do tej pory reguły postępowania przestają być respektowane lub okazują się niewystarczające, role procesowe ulegają zaburzeniu. Organizacja podejmuje improwizowane działania, by przywrócić stan sprzed katastrofy. Pojawia się chaos i szukanie rozwiązań na siłę. Bez odpowiedniego wcześniejszego przygotowania trudno jest zapewnić funkcjonowanie organizacji na akceptowalnym poziomie.

By zapewnić firmie nieprzerwaną realizację założonych celów i strategii biznesowych oraz funkcjonowanie procesów mimo pojawiających się negatywnych okoliczności i zdarzeń, konieczne jest skonstruowanie takich mechanizmów, które tę nieprzerwaną działalność zagwarantują. Główny etap zarządzania ciągłością działania to jednak nie, jak by się mogło wydawać, realizacja działań w trakcie wystąpienia zakłóceń działalności organizacji, lecz przede wszystkim czynności prewencyjne odnoszące się do zapobieżenia wystąpienia sytuacji kryzysowej oraz planowanie, zgrywanie i doskonalenie działań mających stanowić szybką odpowiedź na ewentualne zakłócenia. Wszystko po to, by zapewnić wysoką odporność na zakłócenia oraz zdolność do szybkiego dostosowania się i odzyskiwania funkcjonowania. Idealny bowiem

plan ciągłości działania to taki, który nigdy nie doczeka się potrzeby operacyjnego uruchomienia.

3. Podłoże do wdrożenia systemu zarządzania ciągłością działania.

Zarządzanie Ciągłością Działania to kompleksowy zestaw działań związanych m.in. z zarządzaniem bezpieczeństwem fizycznym, bezpieczeństwem informacji, zarządzaniem ryzykiem operacyjnym, zarządzaniem kryzysowym, przywracaniem zasobów (w tym systemów IT) po katastrofie czy odtwarzania danych.



Na gruncie polskim, na regulacje w zakresie zarządzania ciągłością działania można natrafić w niektórych polskich ustawach, m.in. w Ustawie o krajowym systemie cyberbezpieczeństwa, Ustawie o zarządzaniu kryzysowym, Ustawie Prawo bankowe, Ustawie Prawo telekomunikacyjne. Kwestie ciągłości działania są też prezentowane w ramach Narodowych Standardów Cyberbezpieczeństwa tj.: NSC 800—34, Poradnik planowania awaryjnego — na podstawie NIST SP 800—34. Najbardziej jednak rozpoznawalne wytyczne dotyczące systemowego zarządzania bezpieczeństwem informacji zostały zmaterializowane w międzynarodowej normie EN ISO 22301:2019 przyjętej przez Polski Komitet Normalizacyjny jako polska norma PN—EN ISO 22301:2020—04. Bezpieczeństwo i odporność — Systemy zarządzania ciągłością działania—Wymagania.

4. Koncepcja zarządzania ciągłością działania wg wymagań Normy ISO 22301.

W normie ISO 22301 określono strukturę oraz wymagania dotyczące wdrożenia i utrzymania

systemu zarządzania ciągłością działania (BCMS), adekwatnego do wielkości i rodzaju wpływu, jaki organizacja może albo zaakceptować po wystąpieniu zakłócenia.

Jak czytamy w normie, wyniki utrzymania BCMS są kształtowane przez wymagania prawne, regulacyjne, organizacyjne i branżowe, wymagania organizacji, dostarczane wyroby i usługi, stosowane procesy, wielkość i strukturę organizacji oraz wymagania stron zainteresowanych.

Norma podkreśla, że wdrożenie BCMS wymaga:

- zrozumienia potrzeb organizacji oraz konieczności ustanowienia polityki i celów ciągłości działania;
- eksploatacji i utrzymania procesów, możliwości i struktur reagowania w celu zapewnienia, że organizacja przetrwa zakłócenia;
- monitorowania oraz przeglądania efektów działania i skuteczności BCMS;
- ciągłego doskonalenia na podstawie wyników pomiarów jakościowych i ilościowych.

Opisane w normie wymagania dotyczące wdrożenia BCMS, podobnie jak przy innych systemach zarządzania ISO opierają się na cyklu PDCA (Planuj — Wykonaj — Sprawdź — Działaj).

5. Elementy systemu zarządzania ciągłością działania.

Struktura normy jest znana z innych norm systemowych rodziny ISO takich jak ISO 9001, ISO/IEC 27001, ISO 14001 co w przypadku wdrożonego w organizacji innego systemu zarządzania w dużym stopniu upraszcza sprawę jej implementacji oraz umożliwia zintegrowanie z funkcjonującymi już systemami zarządzania. BCMS opisany przez normę zawiera typowe dla systemów zarządzania ISO elementy, takie jak:

- a) polityki;
- b) kompetentni pracownicy z określonymi odpowiedzialnościami;
- c) procesy zarządzania dotyczące:
 - polityki;
 - planowania;
 - wdrażania i działań operacyjnych;
 - oceny efektów działania;
 - przeglądu zarządzania;
 - ciągłego doskonalenia;
- d) udokumentowane informacje wspomagające

nadzór działań operacyjnych i umożliwiających ocenę efektów działania.

Poszczególne rozdziały normy, korespondują z etapami cyklu PDCA:

- Rozdział 4 zawiera wymagania niezbędne do ustanowienia kontekstu BCMS;
- Rozdział 5 to przede wszystkim wymagania określone dla najwyższego kierownictwa;
- Rozdział 6 zawiera wymagania dotyczące ustanowienia celów strategicznych i głównych zasad dla BCMS;
- Rozdział 7 podnosi kwestie działań związanych z ustanowieniem i podnoszeniem kompetencji oraz komunikacją i dokumentowaniem;
- Rozdział 8 określa planowanie potrzeb w zakresie ciągłości działania, a także sposoby opracowania procedur zarządzania organizacją w razie wystąpienia zakłócenia;
- Rozdział 9 to wymagania niezbędne do pomiaru efektów działania oraz do przeprowadzenia przeglądu zarządzania;
- Rozdział 10 odnosi się do działań w zakresie niezgodności BCMS i ciągłego doskonalenia.

**Dowiedz się więcej
o zarządzaniu ciągłością
działania (PN-EN ISO
22301:2020). Kliknij i sprawdź!**

6. Działania operacyjne w Systemie Zarządzania Ciągłością Działania.

Zarządzanie organizacją w sytuacji kryzysowej wymaga zaplanowania szeregu działań operacyjnych uwzględniających zarówno kontekst organizacji, jak i działań odnoszących się do ryzyk i szans. W punkcie 8 normy wyszczególniono wymagania w zakresie działań operacyjnych niezbędnych do wdrożenia skutecznego systemu zarządzania ciągłością działania. Należą do nich:

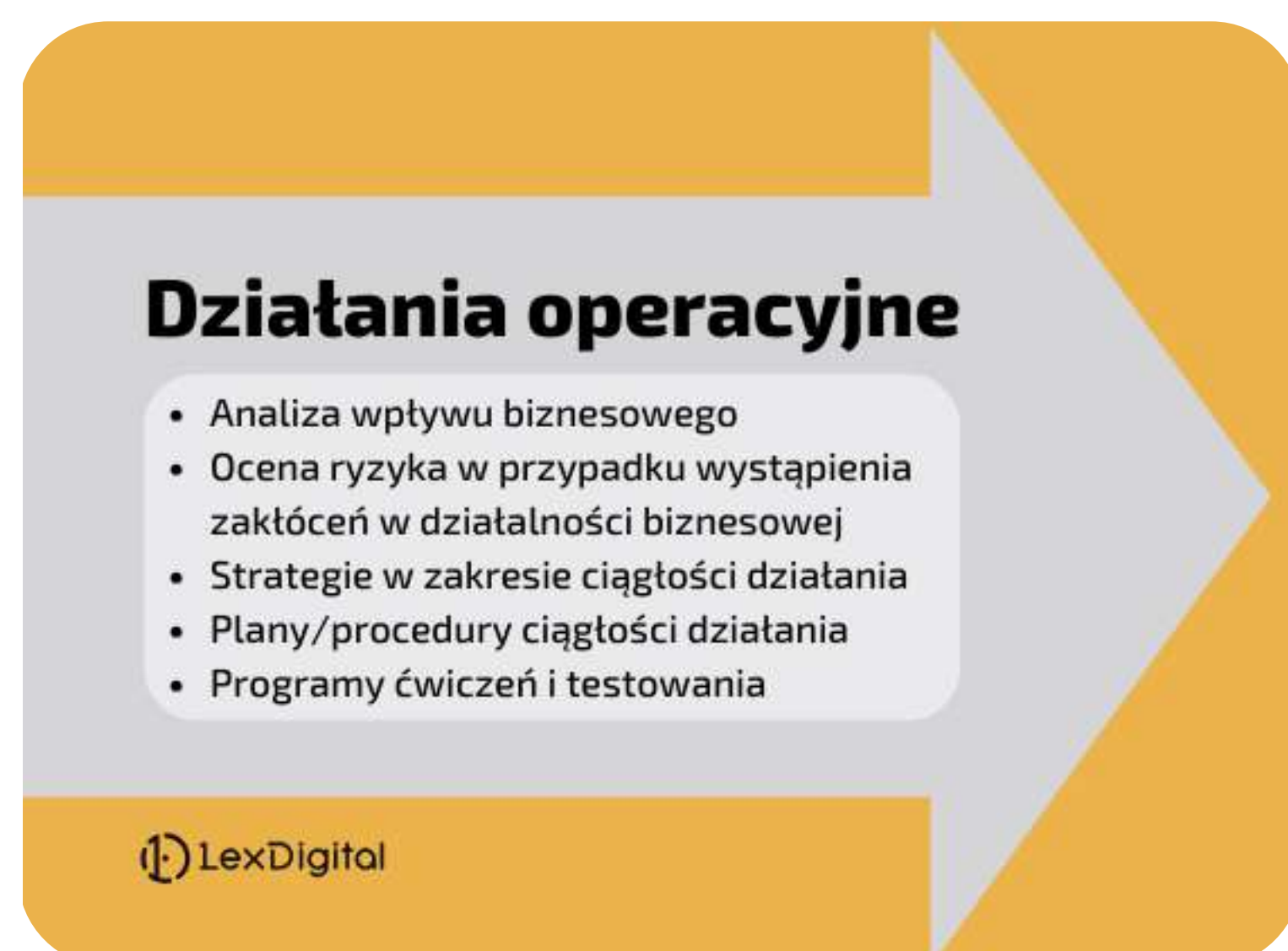
- **Analiza wpływu biznesowego (BIA)** — której zadaniem jest określenie priorytetów i wymagań w zakresie ciągłości działania. Organizacja poprzez analizę BIA winna wytypować procesy krytyczne dla jej funkcjonowania, które mają wpływ na dostarczanie wyrobów i usług. Analiza

BIA powinna identyfikować także ramy czasowe i związane z tym poziomy akceptowalności niewznowienia działań przy pomocy takich parametrów jak:

- MTPD — maksymalny tolerowany okres zakłócenia;
- RTO — czas wznowienia działania.

Wynikiem analizy BIA winno być wskazanie działań priorytetowych z uwzględnieniem zasobów i zależności w zakresie realizacji priorytetowych działań.

- **Ocena ryzyka w przypadku wystąpienia zakłóceń w działalności biznesowej** — w tym wskazanie ryzyk zakłóceń dla kluczowych procesów i działań, dokonanie ich analizy i oceny oraz podjęcie decyzji co do postępowania z ryzykami.
- **Strategie w zakresie ciągłości działania** — mające za zadanie oddziaływać na prawdopodobieństwo, czas trwania, a także wpływ zakłócenia na wyroby i usługi.
- **Plany/procedury ciągłości działania** — dokumentujące takie elementy jak struktura reagowania kryzysowego, procedury postępowania, działania w zakresie ostrzegania i komunikacji, szczegóły realizowanych działań z przypisaniem odpowiedzialności za ich realizację, uwzględnienie wykorzystania niezbędnych zasobów czy sprawozdawczość i odtwarzanie.
- **Programy ćwiczeń i testowania** — działania zgrywające i doskonalące poszczególne elementy strategii i przyjętych rozwiązań.



Właściwe przygotowanie działań operacyjnych, które zapewnią ostateczny efekt, wymagają

zaangażowania interdyscyplinarnego całej organizacji. Elementy istotne w procesie zachowania ciągłości działania to m.in. elementy organizacyjne i zarządcze w tym odpowiednia struktura zarządzania w czasie kryzysu, współdziałanie poszczególnych pionów organizacyjnych, aktywa techniczne – ich wydolność, zastępowalność i zapewnienie możliwości ich odtworzenia, zagadnienia logistyczne – związane z zapewnieniem alternatywnej lokalizacji dla poszczególnych elementów infrastruktury oraz ich ewakuacji i przemieszczenia, prawne – związane np. z kwestią ochrony przed roszczeniami, komunikacyjne – dotyczące wymiany informacji z interesariuszami, służbami i organami Państwa.

7. Korzyści z wdrożenia Systemu Zarządzania Ciągłością Działania.

Korzyści dotyczące wdrożenia i utrzymania rozwiązań zapewniających ciągłość działania organizacji są wielowymiarowe. Skutecznie działający BCMS może być substytutem ubezpieczenia się od negatywnych zdarzeń, które mogą dotyczyć organizację.

Doświadczenia ostatnich lat dobitnie pokazują, że wszystko się może zdarzyć a sytuacje kryzysowe, których wcześniej nie traktowano w kategoriach ryzyk takie jak utrata personelu, przerwy w funkcjonowaniu na skutek pandemii, a także klęski żywiołowe spowodowane nagłymi zjawiskami atmosferycznymi czy zagrożenia wojenne są jak najbardziej realne. Biorąc powyższe okoliczności pod uwagę, do głównych korzyści związanych z wdrożeniem BCMS zaliczyć można:

- uporządkowanie procesów w organizacji;
- wyeliminowanie podatności i słabości w działaniach operacyjnych;
- stwarzanie warunków do zapewnienia przewagi konkurencyjnej;
- zmniejszenie ryzyka potencjalnych strat finansowych lub całkowitego zaprzestania działalności;
- zapewnienie wzmocnienia wiarygodności organizacji i reputacji w oczach stron trzecich;
- ochronę podstawowych wartości takich jak zdrowie czy życie ludzkie;
- stwarzanie perspektywy do dalszego rozwoju.

POTRZEBUJESZ POMOCY Z NORMAMI ISO? ZGŁOŚ SIĘ DO NAS!

Odpowiemy na nurtujące Cię pytania, zaplanujemy spotkanie, przygotujemy spersonalizowaną ofertę dopasowaną do potrzeb Twojej organizacji.

E-mail: biuro@lexdigital.pl

Tel.: +48 500 214 942



Prasówka



Dane biometryczne w pracy: nowy przewodnik hiszpańskiej agencji ochrony danych

23 listopada 2023 r. Hiszpańska Agencja Ochrony Danych (AEPD) opublikowała „Przewodnik po zabiegach kontroli obecności za pomocą systemów biometrycznych”, ustanawiający kryteria stosowania danych biometrycznych do kontroli dostępu, zarówno w kontekście pracy, jak i poza nią. W przewodniku przedstawiono środki zapewniające, że przetwarzanie danych osobowych przy użyciu tej technologii jest zgodne z ogólnym rozporządzeniem o ochronie danych (RODO) i innymi właściwymi przepisami.

W dyrektywie AEPD dostrzega się szybką ewolucję systemów biometrycznych i przetwarzania danych, podkreślając charakter wysokiego ryzyka związanego z przetwarzaniem danych biometrycznych w celu identyfikacji i uwierzytelniania. Takie przetwarzanie wiąże się ze szczególnymi kategoriami danych, a RODO wymaga szczególnych okoliczności i warunków uzasadniających ich przetwarzanie.

W przypadku czynności związanych z miejscem pracy, takich jak mierzenie czasu i kontrola dostępu, w poradniku wskazano, że zniesienie zakazu przetwarzania danych biometrycznych (zgodnie z art. 9 ust. 2 lit. b RODO) wymaga normy prawnej zezwalającej na wykorzystanie takich danych. Zgoda nie może być podstawą legalności ze względu na brak równowagi pomiędzy osobą poddawaną leczeniu a podmiotem go przeprowadzającym.

W przypadku kontroli dostępu niezwiązanej z pracą zgoda nie jest również wystarczająca do

zniesienia zakazu ze względu na obarczony wysokim ryzykiem charakter leczenia i niespełnienie warunku konieczności (art. 35 ust. 7 lit. b).

Przewodnik nakłada ograniczenia na zabiegi biometryczne polegające na zautomatyzowanym podejmowaniu decyzji bez interwencji człowieka, szczególnie gdy ma to istotny wpływ na jednostkę. Podkreśla on obowiązkowy charakter oceny skutków dla ochrony danych przed rozpoczęciem przetwarzania danych biometrycznych, wykazując przydatność, konieczność i proporcjonalność.

Dodatkowo, jeśli zapewniona zostanie zgodność z zasadami RODO, w poradniku wymieniono środki, które należy wdrożyć, m.in. informowanie osób o zabiegu, umożliwienie unieważnienia powiązania tożsamości, zapewnienie środków technicznych uniemożliwiających nieuprawnione wykorzystanie, stosowanie szyfrowania w celu ochrony danych oraz usuwanie danych biometrycznych niezwiązanych z tego cel. W przewodniku podkreślono znaczenie ochrony danych już na etapie projektowania i zaleca się minimalizację gromadzonych danych, obiektywnie oceniając brak przetwarzania danych specjalnej kategorii.

Źródło: <https://bit.ly/3v337PN>

Naukowcy z jednostki Google DeepMind znaleźli jeszcze prostszy sposób na przetwarzanie wyrównania ChatGPT OpenAI

Wpisując polecenie w monicie i prosząc ChatGPT o powtarzanie słowa, takiego jak "wiersz" bez końca, naukowcy odkryli, że mogą zmusić program do

wypłucia całych fragmentów literatury, które zawierały jego dane szkoleniowe, nawet jeśli tego rodzaju wyciek nie powinien mieć miejsca w przypadku wyrównanych programów. Naukowcy nazywają to zjawisko "wyodrębnialnym zapamiętywaniem", które jest atakiem, który zmusza program do ujawnienia rzeczy przechowywanych w pamięci.

Znaleźli także dane osobowe dziesiątek osób. Spośród 15 000 prób ataków około 17% zawierało "zapamiętane dane osobowe", takie jak numery telefonów. Autorzy starają się określić ilościowo, ile danych szkoleniowych może wyciekać. Znaleźli duże ilości danych, ale wyszukiwanie jest ograniczone faktem, że prowadzenie eksperymentu, który może trwać i trwać, kosztuje.

Dzięki powtarzającym się atakom znaleźli 10 000 instancji "zapamiętanej" treści ze zwracanych zestawów danych. Stawiają hipotezę, że można znaleźć znacznie więcej, jeśli ataki będą kontynuowane. Piszą, że eksperyment porównywania danych wyjściowych ChatGPT z zestawem AUXDataSet został uruchomiony na jednej maszynie w Google Cloud przy użyciu procesora Intel Sapphire Rapids Xeon z 1,4 terabajta pamięci DRAM. Prowadzenie zajęło tygodnie. Ale dostęp do mocniejszych komputerów może pozwolić im na szersze testowanie ChatGPT i znalezienie jeszcze większej liczby wyników.

"Przy naszym ograniczonym budżecie wynoszącym 200 USD wyodrębniliśmy ponad 10 000 unikalnych przykładów" - piszą Nasr i zespół. "Jednak przeciwnik, który wydaje więcej pieniędzy na zapytanie o interfejs API ChatGPT, może prawdopodobnie wyodrębnić znacznie więcej danych."

Źródło: <https://zd.net/3Tl67kD>



Google otwiera Centrum Cyberbezpieczeństwa w Maladze

Google zapoczątkował nowe Centrum Inżynierii Bezpieczeństwa (GSEC) na hiszpańskim wybrzeżu, skupiając się na zwalczaniu rosnących zagrożeń cybernetycznych. Kent Walker, prezes ds. spraw globalnych Google & Alphabet, podkreśla, że zagrożenia stają się bardziej wyrafinowane, kosztowne i agresywne, co podkreśla znaczenie budowy bezpiecznego Internetu. GSEC w Maladze będzie gromadzić zespoły i ekspertów, pracujących nad nowoczesnymi badaniami i narzędziami opartymi na szybkości, otwartym kodzie źródłowym i sztucznej inteligencji.

Centrum nie tylko skupi się na badaniach, ale również będzie oferować przestrzeń szkoleniową, organizując spersonalizowane warsztaty dla różnych grup, w tym urzędników państwowych, przedsiębiorstw i osób poszukujących pracy. Inicjatywa jest częścią dążenia Google do podniesienia standardów bezpieczeństwa w erze rozwijających się zagrożeń cybernetycznych. Przy wsparciu finansowym w postaci 10 milionów dolarów przekazanych przez Google.org, firma wspiera także rozwój szkoleń z zakresu umiejętności cyberbezpieczeństwa, z myślą o lokalnych organizacjach społecznościowych.

Źródło: <https://bit.ly/3RBjc8o>

Orzeczenie TSUE w sprawie kar pieniężnych

5 grudnia 2023 roku Trybunał Sprawiedliwości Unii Europejskiej stwierdził, że administracyjną karę pieniężną można nałożyć jedynie w przypadku umyślnego lub nieumyślnego naruszenia. Istotne jest, że karę można nałożyć na osobę prawną, niezależnie od tego, czy naruszenie popełnił organ zarządzający czy ktoś inny w ramach działalności firmy. TSUE podkreślił również możliwość karania za operacje dokonywane przez podmiot przetwarzający, jeśli można je przypisać administratorowi.

TSUE odniósł się do dwóch przypadków - litewskiego i niemieckiego. Litewska sprawa dotyczyła krajowego centrum zdrowia publicznego,

które zostało ukarane za utworzenie aplikacji monitorującej dane osób narażonych na COVID-19. Niemiecka sprawa dotyczyła firmy Deutsche Wohnen, której nałożono karę za przechowywanie danych osobowych najemców dłużej niż konieczne. TSUE podkreślił, że administracyjne kary pieniężne można nałożyć tylko w przypadku naruszenia zawinionego, a odpowiedzialność za nie spoczywa na osobie prawnej, niezależnie od tego, czy naruszenie popełnił organ zarządzający czy ktoś inny działający na rachunek firmy. Trybunał zaznaczył również, że współadministrowanie danych nie wymaga formalnych uzgodnień, a wystarczające są wspólne lub zbieżne decyzje między podmiotami.

Źródło: <https://bit.ly/3RDZtor>

Scoring to zautomatyzowane podejmowanie decyzji według TSUE

RODO sprzeciwia się dwóm praktykom biur informacji kredytowej, zwłaszcza niemieckiemu SCHUFA. Trybunał Sprawiedliwości Unii Europejskiej (TSUE) rozpatrzył sprawę, gdzie scoring, czyli matematyczna metoda przy ocenie zdolności kredytowej, został uznany za zautomatyzowane podejmowanie decyzji, co jest w zasadzie zakazane przez RODO. Niemiecki sąd musi teraz ocenić, czy istnieje wyjątek od tego zakazu.

TSUE także stwierdził, że przechowywanie informacji o zwolnieniu z pozostałej części długu przez biura kredytowe dłużej niż sześć miesięcy jest sprzeczne z RODO. Wartość zwolnienia z długu dla ponownego uczestnictwa w życiu gospodarczym jest kluczowa. Niemieckie biura przechowują te dane przez trzy lata, podczas gdy publiczny rejestr upadłości przewiduje sześciomiesięczny okres przechowywania. Po tym czasie prawa i interesy osoby mają pierwszeństwo. Osoba, której dane dotyczą, ma prawo do usunięcia nielegalnie przechowywanych danych. TSUE podkreślił też, że sądy krajowe powinny kontrolować decyzje organów nadzorczych, a osoba dotknięta decyzją ma prawo sprzeciwić się przetwarzaniu swoich danych i do ich usunięcia, chyba że istnieją nadrzędne prawnie uzasadnione podstawy.

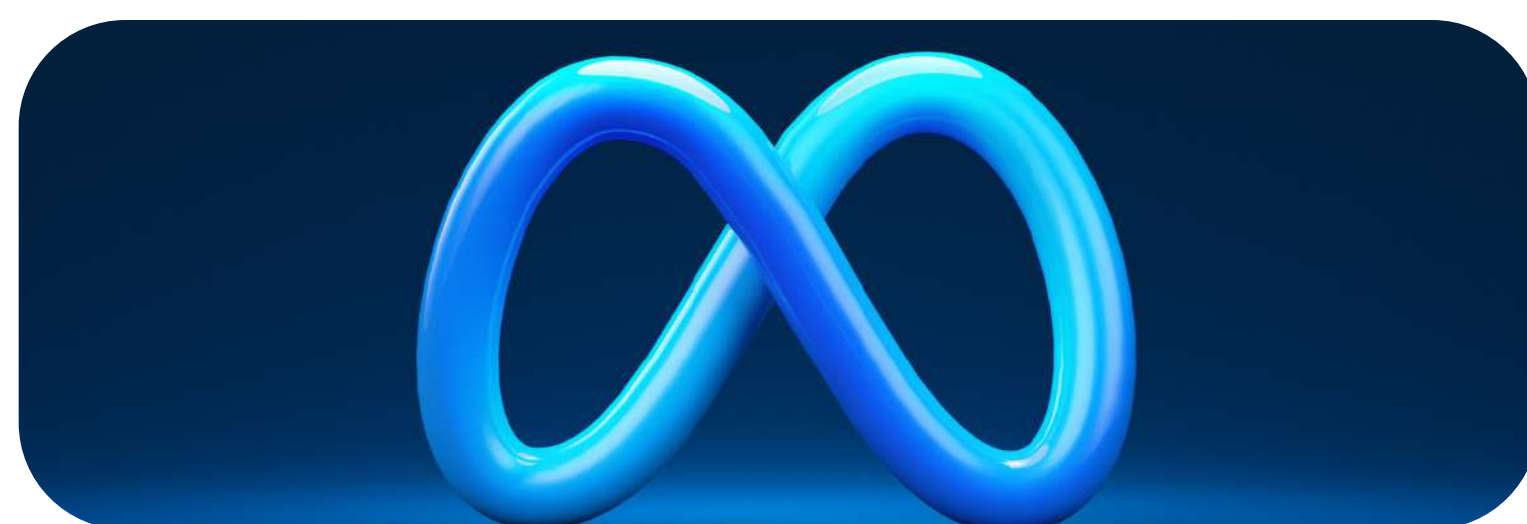
Źródło: <https://bit.ly/487yYhf>

Meta znowu podpadła Noyb. Tym razem chodzi o płatność za zachowanie prywatności

Meta znalazła się w centrum uwagi po złożeniu skargi przez grupę ds. ochrony danych osobowych Noyb, oskarżającej firmę o naruszenie europejskiego prawa o ochronie danych. Skarga wynika z nowej polityki Meta, która oferuje użytkownikom wybór między akceptacją spersonalizowanych reklam opartych na danych osobowych a opłatą do 250 euro rocznie za wersję bez reklam.

Grupa Noyb, kierowana przez prawnika-aktywistę Maxa Schremsa, domaga się pilnego dochodzenia w sprawie Meta oraz nakładania grzywny, aby odstraszyć inne firmy od stosowania podobnych praktyk. Spór koncentruje się na pytaniu, czy Meta może uzyskać legalną zgodę na przetwarzanie danych, gdy jedyną alternatywą jest płatność za zachowanie prywatności.

Skarga argumentuje, że wprowadzenie opłat za ochronę prywatności ogranicza dostęp do podstawowego prawa każdemu, kto nie może sobie na to pozwolić.



W skardze zarzuca się, że opłaty Facebooka są „wyraźnie zawyżone” i stanowią „opłatę za prywatność”. Facebook pobierze od użytkowników opłatę w wysokości do 12,99 euro, a każde połączone konto będzie kosztować kolejne 8 euro, co stanowi równowartość do 250 euro rocznie na jedną osobę korzystającą Instagram i Facebook. Dla porównania, według szacunków sporządzonych na podstawie danych Meta, średni roczny przychód, jaki Meta otrzymuje od każdego użytkownika w Europie, wynosi 63 euro.

Meta stwierdziła, że ceny jej subskrypcji są porównywalne z cenami innych usług internetowych, takich jak usługa wideo YouTube Premium, usługa strumieniowego przesyłania muzyki Spotify i usługa strumieniowego przesyłania filmów Netflix.

Felix Mikolasch, prawnik ds. ochrony danych w firmie Noyb, powiedział: „Prawo UE wymaga, aby zgoda była rzeczywiście wolną wolą użytkownika. Wbrew temu prawu Meta pobiera „opłatę za ochronę prywatności” w wysokości do 250 euro rocznie, jeśli ktokolwiek ośmieli się skorzystać ze swojego podstawowego prawa do ochrony danych.

Źródło: <https://bit.ly/46VJarE>

Nuklearne kłopoty: ataki hackerów na brytyjską stronę

Sellafield, najbardziej niebezpieczny brytyjski zakład nuklearny, padł ofiarą cyberataków związanych z Rosją i Chinami – donosi The Guardian. Ataki, odkryte po raz pierwszy w 2015 roku, były tuszowane przez kierownictwo, co rodzi obawy o konsekwencje. Ostateczny zakres incydentu i usunięcie malware pozostają niepewne, a kluczowe operacje, takie jak obsługa odpadów radioaktywnych, mogły być zagrożone. Zwłoka w zgłaszaniu naruszeń utrudniła ocenę skali straty danych. Sellafield, o powierzchni 6 km², przechowuje znaczną ilość plutonu i odpadów nuklearnych, będąc jednym z najniebezpieczniejszych miejsc na świecie.

Urząd ds. Regulacji Nuklearnej (ONR) potwierdził, że Sellafield nie spełnia norm cyberbezpieczeństwa, a w zeszłym roku trafiła pod "specjalne środki" za stałe braki w tej dziedzinie. Są podejrzenia o planowane ściganie jednostek na miejscu. Problemy z cyberbezpieczeństwem w Sellafield są znane od co najmniej dekady, a raport z 2012 roku alarmował, że istnieją "krytyczne podatności". ONR przygotował zawiadomienie o karze za cyberbezpieczeństwo, wskazując na "dostateczne dowody na skazanie".

Odkrycia te pojawiają się w kontekście rosnących obaw dotyczących cyberataków na infrastrukturę. GCHQ ostrzega przed zwiększonym ryzykiem cyberataków ze strony Rosji i Chin. Sellafield przechowuje kluczowe dokumenty dotyczące awaryjnych protokołów nuklearnych, których ujawnienie byłoby niebezpieczne. ONR był zaniepokojony możliwością zewnętrznego dostępu do serwerów Sellafield i rzekomego tuszowania, przeprowadzając rozmowy pod ostrzeżeniem. Cyberbezpieczeństwo w Sellafield jest uważane za niewystarczające, a śledztwo The Guardian sugeruje, że kierownictwo celowo ukrywało skalę problemów przed kontrolerami bezpieczeństwa.

Źródło: <https://bit.ly/4ageNio>





Polska

PUODO nałożył administracyjną karę pieniężną w wysokości 103.752 PLN na firmę Link4 Towarzystwo Ubezpieczeń S.A. z Warszawy za naruszenie przepisu RODO. Firma nie zgłosiła organowi nadzorczemu, czyli Prezesowi UODO, naruszenia ochrony danych osobowych w terminie 72 godzin od jego stwierdzenia, co stanowiło naruszenie art. 33 ust. 1 rozporządzenia 2016/679.

Sprawa dotyczyła udostępnienia nieuprawnionemu odbiorcy potwierdzenia przyznania odszkodowania, zawierającego dane osobowe. Informacja ta została przesłana w wyniku błędu ludzkiego do nieuprawnionego odbiorcy wraz z danymi dotyczącymi szkody samochodowej. Pomimo wiedzy Administratora o zdarzeniu, firma nie poinformowała UODO o incydencie, co doprowadziło do wszczęcia postępowania administracyjnego.

Link4 argumentowało, że ryzyko naruszenia było niskie, co uzasadniało niezgłaszanie incydentu. Jednakże Prezes UODO uznał, że udostępnienie danych osobowych nieuprawnionemu odbiorcy stanowiło naruszenie, a firma powinna było zgłosić je organowi nadzorczemu.

Źródło: <https://bit.ly/3TIYKJU>

Świat

Włoski organ ochrony danych nałożył na administratora, podmiot świadczący opiekę zdrowotną, karę w wysokości 40 000 euro zgodnie z art. 83 ust. 4 RODO i art. 83 ust. 5 RODO. Niektórzy z pracowników administratora mogli uzyskać dostęp do dokumentacji zdrowotnej innych współpracowników bez zgody, naruszając jednocześnie niektóre zasady przetwarzania danych zgodnie z art. 5 ust. 1 RODO.

Sprawa dotyczy pracownika Terytorialnego Urzędu ds. Zdrowia Społecznego w Lodi, który złożył skargę do włoskiego organu ochrony danych (DPA) po odkryciu, że w latach 2019–2020 współpracownicy wielokrotnie uzyskiwali dostęp do jej dokumentacji zdrowotnej. Współpracownicy twierdzili, że uzyskali

dostęp do plików, aby ustalić, na których lekarzach mogą polegać w zakresie leczenia pacjentów podczas pandemii Covid-19. Administrator argumentował, że dostęp dotyczył zadań instytucjonalnych związanych ze zdrowiem publicznym, powołując się na dorozumianą zgodę.

Organ ochrony danych zbadał i stwierdził, że dostęp do dokumentacji zdrowotnej pracownika był niezgodny z prawem, naruszał zasady legalności, celowości, przejrzystości, uczciwości i minimalizacji danych zgodnie z RODO. Organ ochrony danych skrytykował także administratora za nieuwzględnienie ryzyka związanego z operacjami przetwarzania danych, naruszenie zasad integralności i poufności. Ponadto DPA stwierdził, że powołanie się przez administratora na art. 17-bis dekretu z mocą ustawy nr 2007/2015 z dnia 20 grudnia 2010 r. Ustawa nr 18/2020 dotycząca zgody dorozumianej była błędna, gdyż nie pozwala na odstępstwa od zasad ochrony danych. Organ ochrony danych podkreślił, że wymagana jest wyraźna zgoda, której w tym przypadku nie uzyskano.

Źródło: <https://bit.ly/4aixCkS>

Region Lombardii, pełniący rolę administratora danych, omyłkowo opublikował na swojej oficjalnej stronie internetowej dane osobowe około 732 pracowników, w tym wrażliwe informacje dotyczące zdrowia. Dwa stowarzyszenia związków zawodowych zwróciły na to uwagę włoskiego organu ochrony danych (DPA). Administrator argumentował, że publikacja była zgodna z wymogami przejrzystości wynikającymi z dekretu legislacyjnego nr 33/2013 oraz że nie przetwarza danych jako pracodawca, ale w celu wypełnienia obowiązków związanych z publikowaniem danych o transakcjach pomiędzy podmiotami prawnymi. Administrator wspomniał również o wyzwaniach związanych z pandemią mających wpływ na jego wydajność.

Włoski organ ochrony danych uznał przetwarzanie za nielegalne, zauważając, że chociaż przetwarzanie danych dotyczących zdrowia w interesie publicznym jest dozwolone, rozpowszechnianie takich

wrażliwych informacji jest sprzeczne z zasadami minimalizacji danych określonymi w art. 5 RODO. Organ ochrony danych odrzucił twierdzenie administratora dotyczące obowiązków w zakresie przejrzystości, podkreślając, że przepisy nie zezwalają na szerszą publikację danych osobowych, zwłaszcza danych dotyczących stanu zdrowia. Organ ochrony danych stwierdził naruszenia art. 5 RODO, art. 6 ust. 1 lit. c) RODO i art. 9 RODO.

Organ ochrony danych wziął pod uwagę czas trwania nielegalnego rozpowszechniania danych i uznając czynniki łagodzące, takie jak niezwłoczne podjęcie działań w celu usunięcia danych i wyzwanie związane z pandemią, nałożył karę w wysokości 20 000 euro, stwierdzając, że okoliczności te nie zwalniają administratora z odpowiedzialności za przestrzeganie przepisów dotyczących ochrony danych.

Źródło: <https://bit.ly/46TJcA3>

Szwedzki organ ochrony danych nałożył karę na Radę ds. Dzieci i Edukacji w Östersund w wysokości 300 000 SEK (około 26 524 EUR) za naruszenie art. 35 ust. 1 RODO.

Rada nie przeprowadziła oceny wpływu na ochronę danych przed rozpoczęciem korzystania z Google Workspace w szkołach.

W Östersund w Szwecji od 2020 r. dwadzieścia cztery szkoły korzystają z Google Workspace do komunikacji, nauczania i odrabiania zadań domowych, przetwarzając dane osobowe 1303 pracowników i 5945 uczniów. Rada ds. Dzieci i Edukacji w Östersund zintegrowała Google Workspace bez przeprowadzania nowej oceny skutków w 2020 r., opierając się na ocenie przeprowadzonej w 2014 r. przez inny podmiot.

Organ ochrony danych zauważył, że przetwarzanie wiązało się z wysokim ryzykiem, zwłaszcza że osobami, których dane dotyczą, były liczne dzieci. Powołując się na przepisy RODO, DPA stwierdził, że w przypadku przetwarzania obarczonego wysokim ryzykiem konieczne są oceny skutków. Pomimo ciągłych wysiłków działania administratora po 2020 r. uznano za niewystarczające, ponieważ powinny były zostać wdrożone przed skorzystaniem z usługi, a przedłużające się opóźnienie w ukończeniu oceny skutków świadczyło o trwałym zaniedbaniu.

Źródło: <https://bit.ly/3ToQLM7>

Newsletter RODO

Listopad 2023 nr 4/2023

Dziękujemy za przeczytanie naszego Newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI