



Pracownicy a cyberbezpieczeństwo

Edukacja pracowników jest kluczowa

Outsourcing kadrowo-płacowy

ESG – co trzeba o nim wiedzieć

Restrukturyzacja zatrudnienia

Ochrona przeciwpożarowa
w zakładzie pracy



Cyberbezpieczeństwo nowa usługa SEKA S.A.

JAROSŁAW GRABOWSKI
PREZES ZARZĄDU SEKA S.A.

STRONA: **4**

Edukacja pracowników jest kluczowa

MARCIN MARCZEWSKI, CEO RESILIA SP. Z O.O.
BARTOSZ SADKOWSKI, COO RESILIA SP. Z O.O.

STRONA: **6**

Rozwiązania skrojone na miarę

ELŻBIETA ZADROŻNA
CZŁONEK ZARZĄDU DS. FINANSOWYCH SEKA S.A.

STRONA: **12**

ESG – co trzeba o nim wiedzieć

EWA CHODOWSKA
EKSPERTKA ESG, MENTORKA NOWEGO KURSU
SEKA „MANAGER ESG”

STRONA: **16**

Kaucja wraca

ALEKSANDER FLOREK
ZASTĘPCA DYREKTORA DZIAŁU HANDLOWEGO
DS. OCHRONY ŚRODOWISKA SEKA S.A.

STRONA: **22**

Sprawniejsza praca

EWA KLIMCZUK
GENERAL MANAGER, EUVIC

STRONA: **26**

Ciągle się pali!

DR INŻ. JAN KOŁDEJ
KOORDYNATOR DS. NADZORU PPOŻ.
SEKA S.A.

STRONA: **30**

Restrukturyzacja zatrudnienia

ROBERT MALISZEWSKI
DYREKTOR DZIAŁU PRAWA PRACY SEKA S.A.

STRONA: **36**

WYDAWCA: SEKA S.A.
ul. Paca 37, 04-386 Warszawa
tel.: 22 517 88 50 | fax: 22 517 88 87
www.seka.pl, seka@seka.pl
www.facebook.com/SEKAszkolenia
Wszelkie prawa zastrzeżone. SEKA S.A.

REDAKTOR PROWADZĄCY: Maciej Mazerant
WSPÓŁPRACA: Anna Witkiewicz, SEKA S.A.
KOREKTA: Piotr Drozdowicz
OKŁADKA: zdjęcie Getty Images, Unsplash+
REALIZACJA: www.pcontent.pl



Szanowni Państwo!

Od lat towarzyszymy Państwu, dostarczając usługi, które budują bezpieczeństwo pracy i prowadzenia biznesu. W tym numerze chcemy opowiedzieć Państwu o naszych kolejnych krokach naprzód, które wzmacniają kompleksowość naszych usług skupionych wokół bezpieczeństwa.

Z satysfakcją dzielimy się informacją, że teraz możemy zadbać również o cyberbezpieczeństwo Państwa firmy, szkolenia pracowników w tym zakresie oraz zgodność z obowiązującymi przepisami. W temat cyberbezpieczeństwa wprowadzą Państwa: Prezes Zarządu SEKA S.A. Jarosław Grabowski, który wyjaśnia, co nas najbardziej przekonało do wejścia w ten obszar usług, oraz przedstawiciele firmy Resilia, partnera SEKA w zakresie cyberbezpieczeństwa, którzy opowiadają o skali cyberzagrożeń, z jakimi mierzą się dziś firmy, oraz o skutecznych sposobach na budowanie cyberochrony.

Od tego roku zaczyna obowiązywać raportowanie ESG. W związku z nowymi wymaganiami, przygotowaliśmy kurs Manager ESG, który zapewnia kompleksowe przygotowanie do roli menedżera lub koordynatora ESG. O tym, co firmy mogą zyskać dzięki ESG, jakie zadania stoją przed specjalistą z tego zakresu i kto najlepiej sprawdzi się w tej roli, pasjonująco opowiada mentorka naszego kursu.

Ponadto w tym numerze piszemy m.in. o tym, jak w polskich firmach przebiega digitalizacja i na ile jesteśmy otwarci na wprowadzenie do naszych procesów AI. Wyjaśniamy, w jaki sposób outsourcing kadrowo-płacowy może się przyczyniać do budowania przewagi konkurencyjnej. Dostarczamy również niezbędnych informacji o systemie kaucyjnym.

Nie zapominamy też o sytuacjach trudnych. Nasz ekspert od prawa pracy dzieli się z Państwem wiedzą, jak ustalać kryteria doboru pracowników przy kwalifikowaniu ich do zwolnienia podczas restrukturyzacji. A koordynator ds. nadzoru PPOŻ., nawiązując do pożarów z ostatnich miesięcy, przypomina o roli audytów PPOŻ. w budowaniu bezpieczeństwa budynków i innych obiektów.

Życzymy Państwu miłej lektury!



Wcześniejsze numery
magazynu SEKA
można pobrać na stronie
www.magazyn.seka.pl

Cyberbezpieczeństwo

nowa usługa SEKA S.A.

Firma SEKA od wielu lat znana jest z dostarczania rozwiązań i usług z zakresu szeroko rozumianego wsparcia bezpieczeństwa w kontekście prowadzenia biznesu. Audyty i szkolenia z zakresu BHP, PPOŻ., ochrony środowiska, a także kompleksowy outsourcing szkoleń dla pracowników i obsługa kadrowo-płacowa były do tej pory najważniejszymi obszarami naszej działalności. Rynek zmienia się jednak bardzo dynamicznie, a wraz z nim oczekiwania klientów i zagrożenia, na jakie narażeni są pracodawcy i pracownicy. Jedne z najpoważniejszych dotyczą ochrony danych osobowych oraz nieuprawnionego dostępu do danych i zasobów przedsiębiorstwa.

JAROSŁAW GRABOWSKI
PREZES ZARZĄDU SEKA S.A.

W skrócie:

- Dlaczego zdecydowaliśmy się dodać do naszych usług cyberbezpieczeństwo?
- Jakie doświadczenie SEKA S.A. chcemy wykorzystać przy cyberbezpieczeństwie?
- Jak wzmacniamy kompleksowość naszych usług?



”

Wzrost zagrożeń w obszarze cyberbezpieczeństwa w Polsce następuje szybciej, niż dzieje się to na świecie.



Jarosław Grabowski, Prezes Zarządu SEKA S.A.

W odpowiedzi na wymagania rynku i zapytania ze strony naszych klientów zdecydowaliśmy się na rozszerzenie naszej oferty o audyty i szkolenia z zakresu cyberbezpieczeństwa. Z ankiet i badań, jakie przeprowadziliśmy, jasno wynika, że brak świadomości zagrożeń na poziomie pracowników oraz niewiedza, jak im przeciwdziałać, to obecnie jedno z największych problemów dla wielu firm, tuż obok odpowiednich zabezpieczeń na poziomie sprzętu i oprogramowania. W SEKA mamy duże doświadczenie w organizacji szkoleń. Prowadzimy je dla kilkudziesięciu tysięcy pracowników rocznie. Zdecydowaliśmy się więc na wprowadzenie do naszej oferty usług z zakresu cyberbezpieczeństwa, które stają się integralną częścią szerszego portfolio firmy.

Gdy przybywa cyberzagrożeń, rośnie potrzeba kompleksowej cyberochrony

Rozwój w obszarze ochrony danych jest odpowiedzią na coraz większe zapotrzebowanie rynku dotyczące skutecznego i kompleksowego podejścia do usług wsparcia prowadzenia biznesu. SEKA – wraz z renomowanymi partnerami specjalizującymi się w tej

dziedzinie – będzie oferować audyty bezpieczeństwa, szkolenia dla pracowników oraz doradztwo techniczne, które mają na celu nie tylko ochronę przed zagrożeniami, ale także edukację i podnoszenie świadomości na temat współczesnych cyberzagrożeń. Wzrost zagrożeń w obszarze cyberbezpieczeństwa w Polsce następuje nawet szybciej, niż dzieje się to na świecie. Nasz kraj, jako członek Unii Europejskiej i NATO, integruje się w międzynarodowe systemy obrony cybernetycznej, co pomaga w ochronie infrastruktury krytycznej i danych osobowych. Jednak rosnąca liczba cyberataków – w tym zaawansowane ataki ransomware i phishing – pokazuje, że zagrożenia ewoluują, wymagając ciągłej adaptacji i innowacji w zakresie strategii bezpieczeństwa. Polskie firmy i instytucje publiczne coraz częściej stają się celami ataków, co skłania do inwestowania w zaawansowane systemy zabezpieczeń. Rozwój technologii IoT (internet rzeczy) i zwiększająca się liczba połączonych urządzeń skokowo potęgują ilość możliwych zagrożeń.

Wsparcie biznesu zyskuje nowy wymiar

Nasze wejście w ten sektor usług jest odpowiedzią na powyższe zagrożenia. Sektor

usług doradczych i szkoleniowych w Polsce prężnie się rozwija, oferując audyty bezpieczeństwa, doradztwo strategiczne oraz szkolenia dla pracowników. Z racji naszego doświadczenia chcemy pomagać organizacjom w stosowaniu się do nowych przepisów prawnych, takich jak unijna dyrektywa NIS2, która wymaga spełnienia określonych warunków nie tylko przez instytucje rządowe, ale także firmy prywatne przetwarzające dane lub mające wpływ na infrastrukturę krytyczną. Nowe regulacje zaostrzają wymogi dotyczące zarządzania danymi i systemami informatycznymi, wprowadzając obowiązek raportowania incydentów bezpieczeństwa, implementacji odpowiednich środków ochronnych, a także regularnego kształcenia personelu. Szkolenia skoncentrowane na cyberbezpieczeństwie nie tylko podnoszą świadomość pracowników w zakresie zagrożeń, ale również uczą ich, jak reagować w przypadku

ataków oraz jak zapobiegać przyszłym incydentom. Usługi cyberbezpieczeństwa są bezpośrednio związane ze strategią firmy, która ma na celu zapewnienie klientom kompleksowego wsparcia w różnych aspektach prowadzenia działalności gospodarczej. Oprócz ochrony danych SEKA planuje dalsze rozszerzenie swojej dotychczasowej oferty – zwłaszcza w obszarze BHP i ochrony środowiska, gdzie nowe regulacje prawne wymagają szeregu zmian po stronie pracodawców. Dzięki takiemu podejściu SEKA umocni pozycję lidera w dostarczaniu usług wsparcia dla biznesu. W ten sposób odpowiadamy także na potrzeby rynku, który coraz bardziej ceni sobie dostawców mogących oferować kompleksowe i integracyjne usługi, pozwalające skupić się na kluczowych celach biznesowych, bez obaw o aspekty formalnoprawne oraz bezpieczeństwo pracowników i danych. ■

Edukacja pracowników jest kluczowa

Na cyberataki narażone są dziś podmioty działające we wszystkich sektorach gospodarki. Jeśli ataki są skuteczne, mogą paraliżować działanie firm i instytucji, doprowadzić do wycieku wrażliwych danych i narażać na konsekwencje finansowe oraz reputacyjne. Aby tego uniknąć, organizacje powinny zapewnić sobie wielopoziomą cyberochronę łączącą technologię, procesy i edukację pracowników. „Kluczowe jest również stworzenie kultury bezpieczeństwa w firmie, gdzie każdy pracownik czuje się odpowiedzialny za ochronę danych i systemów” – mówią w naszej rozmowie eksperci z firmy Resilia, która jest partnerem SEKA w zakresie cyberbezpieczeństwa: Marcin Marczewski, CEO Resilia, oraz Bartosz Sadkowski, COO Resilia.

MARCIN MARCZEWSKI, CEO Resilia Sp. z o.o.
BARTOSZ SADKOWSKI, COO Resilia Sp. z o.o.,
Partner zarządzający Crawford Polska Sp. z o.o.

W skrócie:

- Na czym dokładnie polega cyberzagrożenie i jakie mogą być konsekwencje cyberataków?
- Jak najczęściej dochodzi do cyberataków i co decyduje o tym, że są skuteczne?
- Jak organizacje powinny dziś dbać o swoje cyberbezpieczeństwo i weryfikować swoje zabezpieczenia?
- Jakie kompetencje powinny rozwijać firmy, które chcą skutecznie chronić się przed cyberzagrożeniami?



PARTNER SEKA S.A.



”

56% firm wskazało, że cyberzagrożenia są bardziej związane z błędami pracowników niż z zaawansowanymi technologiami używanymi przez hakerów, wynika z badań Ponemon Institute.



Coraz częściej słyszymy o cyberatakach. Doszło do nich podczas olimpiady w Paryżu, czasem prowadzą do paraliżu ruchu pociągów czy wycieku wrażliwych danych, np. klientów firm medycznych. Czy jakkolwiek firma czy instytucja może dziś czuć się bezpiecznie?

MM: W dzisiejszych czasach żadna firma ani instytucja nie może czuć się w pełni bezpieczna przed cyberatakami. Coraz częstsze przypadki takich ataków, jak te podczas olimpiady w Paryżu w 2024 roku, pokazują, że cyberprzestępcy mogą zaatakować w dowolnym momencie, niezależnie od skali i rodzaju organizacji. Według raportu IBM Security X-Force, w 2023 roku średni czas wykrycia naruszenia bezpieczeństwa wynosił 207 dni, co wskazuje na to, że firmy mogą być podatne na ataki przez długi czas, zanim zdadzą sobie z tego sprawę. Nawet instytucje z najbardziej zaawansowanymi środkami ochrony muszą być świadome, że zagrożenia ewoluują w tempie, które utrudnia ich pełne zneutralizowanie. Przykład z 2020 roku, gdy atak na firmę SolarWinds wpłynął na bezpieczeństwo tysięcy organizacji

na całym świecie, pokazuje, jak łatwo nawet najbardziej zaawansowane systemy mogą zostać naruszone. Z danych PwC wynika, że ponad 90% dużych firm na świecie doświadczyło co najmniej jednego cyberataku w ciągu ostatnich kilku lat, co tylko podkreśla skalę tego problemu.

Na czym dokładnie polega cyberzagrożenie i jakie mogą być konsekwencje cyberataków, np. dla instytucji, firm produkcyjnych czy usługowych?

BS: Cyberzagrożenia to szerokie spektrum działań skierowanych przeciwko użytkownikom, systemom komputerowym i sieciom, które mają na celu naruszenie ich integralności, poufności lub dostępności. Mogą one przybierać formę ataków z użyciem złośliwego oprogramowania (jak ransomware, spyware), ataków typu DDoS, czy też wyłudzenia danych przez phishing.

Konsekwencje cyberataków mogą być katastrofalne. Dla instytucji publicznych, takich jak szpitale czy urzędy, atak może oznaczać paraliż systemów operacyjnych, a następnie skutkować niemożnością ob-

sługi pacjentów lub obywateli. Na przykład, w 2020 roku atak ransomware na szpital w Niemczech spowodował śmierć pacjenta, ponieważ placówka nie była w stanie przyjąć go na czas ze względu na zablokowane systemy komputerowe. W przypadku firm produkcyjnych skuteczny cyberatak może doprowadzić do przerwania łańcucha dostaw lub uszkodzenia linii produkcyjnych, co prowadzi do ogromnych strat finansowych. W 2017 roku atak ransomware NotPetya sparaliżował działalność takich firm jak Maersk czy Merck, generując straty liczone w miliardach dolarów.

W sektorze usługowym, szczególnie w branży medycznej i finansowej, cyberatak może prowadzić do wycieku najbardziej wrażliwych danych osobowych klientów. Przykład firmy Equifax, która w 2017 roku doświadczyła wycieku danych osobowych ponad 147 milionów klientów, pokazuje, jak poważne mogą być konsekwencje takiego incydentu – zarówno finansowe, jak i reputacyjne.

Czy cyberatak zawsze zostawia ślad? Czy możemy być nieświadomi tego, że np. skradziono nam dane?

MM: Nie każdy cyberatak zostawia wyraźne ślady. Wiele ataków jest tak zaplanowanych, aby działać bez wykrycia przez długi czas. W przypadku zaawansowanych, trwałych zagrożeń (APT), atakujący mogą uzyskać dostęp do systemu i pozostawać w nim niezauważeni przez miesiące, a nawet lata. Jak wskazuje raport firmy FireEye, średni czas, w jakim APT pozostaje niewykryty w systemie, wynosi 205 dni. Możemy być nieświadomi, że nasze dane zostały skradzione, zwłaszcza gdy atakujący nie dokonuje żadnych widocznych zmian w systemie. Przykładem może być przypadek Yahoo!, gdzie atakujący uzyskali dostęp do kont ponad 3 miliardów użytkowników, a incydent ten wyszedł na jaw dopiero kilka lat po fakcie. Takie ataki mogą pozostać niewykryte, dopóki skradzione dane nie zostaną wykorzystane lub sprzedane na czarnym rynku.

Jak najczęściej dochodzi do cyberataków i co decyduje o tym, że są skuteczne?

BS: Najczęściej cyberataki zaczynają się od najprostszej formy manipulacji – socjotechniki, w której ludzie są najsłabszym ogniwem. Phishing, czyli

wyłudzanie informacji (w tym danych dostępowych do konta) za pomocą spreparowanych wiadomości e-mail, jest jednym z najbardziej powszechnych wektorów ataku. Według danych z raportu Verizon Data Breach Investigations Report, aż 85% naruszeń bezpieczeństwa w 2023 roku miało podłoże socjotechniczne, z czego większość była związana z phishingiem. Tu warto zatem wspomnieć o istocie pracy działów HR i innych jednostek odpowiedzialnych za organizację szkoleń w firmach. O skuteczności cyberataków decyduje kilka czynników. Po pierwsze, poziom zaawansowania technicznego i doświadczenie atakujących. Po drugie, istotne znaczenie ma stan zabezpieczeń ofiary – przestarzałe systemy, brak aktualizacji zabezpieczeń czy błędy w konfiguracji aplikacji oraz infrastruktury IT, często otwierają drzwi do ataków. W 2017 roku, podczas ataku ransomware WannaCry, setki tysięcy komputerów na całym świecie zostały zainfekowane z powodu niewdrożenia odpowiednich poprawek bezpieczeństwa.

Jak w takim razie organizacje powinny dziś dbać o swoje cyberbezpieczeństwo i jak weryfikować swoje zabezpieczenia? Możemy być przekonani, że o wszystko zadbałismsy: mamy program antywirusowy, korzystamy z usług wiarygodnych dostawców, mamy wewnętrzne procedury, zespół IT. Czy to dziś wystarczy?

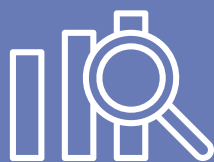
MM: Dbanie o cyberbezpieczeństwo to proces ciągły i wieloaspektowy. Organizacje powinny przyjąć podejście holistyczne, łącząc technologię, procesy i edukację pracowników. Działania techniczne powinny koncentrować się na uwzględnianiu cyberbezpieczeństwa w przygotowaniu, zarządzaniu i utrzymywaniu zasobów IT oraz korzystaniu z nich. Mając podstawową

Konsekwencje cyberataków

Instytucje publiczne – takie jak szpitale czy urzędy, atak może doprowadzić do paraliżu systemów operacyjnych, skutkując niemożnością obsługi pacjentów lub obywateli.

Firmy produkcyjne – skuteczny cyberatak może doprowadzić do przzerwania łańcucha dostaw lub uszkodzenia linii produkcyjnych, co w konsekwencji prowadzi do ogromnych strat finansowych.

Sektor usługowy – szczególnie branża medyczna i finansowa, cyberatak może prowadzić do wycieku najbardziej wrażliwych danych osobowych klientów, wywołując konsekwencje finansowe i reputacyjne.



Skuteczność cyberataków

Ponad 90% dużych firm na świecie doświadczyło co najmniej jednego cyberataku w ciągu ostatnich kilku lat.

O skuteczności cyberataków decyduje m.in. poziom zaawansowania technicznego i doświadczenie atakujących, a także stan zabezpieczeń ofiary – przestarzałe systemy, brak aktualizacji zabezpieczeń czy błędy w konfiguracji aplikacji oraz infrastruktury IT.

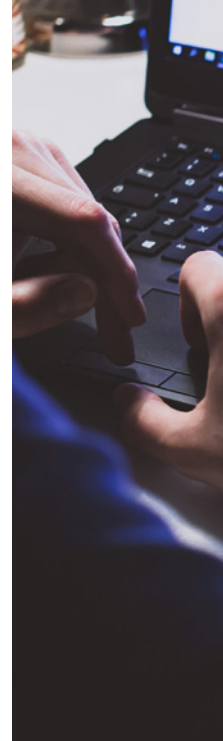
cyberhigienę techniczną i procesową, można planować kolejne zadania w zakresie cyberbezpieczeństwa. Następnym krokiem powinno być regularne przeprowadzanie audytów bezpieczeństwa, które pozwalają zidentyfikować słabe punkty w infrastrukturze IT. Firmy powinny również inwestować w zaawansowane rozwiązania technologiczne, umożliwiające monitorowanie i analizę zdarzeń w czasie rzeczywistym. Ważnym elementem jest także stosowanie testów penetracyjnych, które symulują rzeczywiste ataki, co pozwala na ocenę skuteczności wdrożonych zabezpieczeń. Dzięki testom można zidentyfikować i usunąć słabe punkty, zanim zostaną one wykorzystane przez cyberprzestępców.

Ponadto warto pamiętać o regularnych szkoleniach pracowników, które zwiększają świadomość zagrożeń. Resilia, również we współpracy z SEKA, oferuje szkolenia z zakresu cyberbezpieczeństwa, które pomagają także pracownikom nietechnicznym zrozumieć, jakie są najnowsze zagrożenia i jak im przeciwdziałać. Edukacja to podstawa, ponieważ to pracownicy są często pierwszą linią obrony przed cyberatakami.

Na ile pracownicy mają świadomość, że bezpieczeństwo firmy w dużym stopniu zależy od ich cyfrowych nawyków? I co za tym idzie, jak ważna jest edukacja pracowników w zakresie cyberbezpieczeństwa oraz jakie są najskuteczniejsze metody podnoszenia świadomości w tym obszarze?

BS: Świadomość pracowników w zakresie wpływu ich cyfrowych nawyków na bezpieczeństwo firmy rośnie, ale wciąż jest wiele do zrobienia. W badaniach Ponemon Institute, 56% firm wskazało, że cyberzagrożenia są bardziej związane z błędami pracowników niż z zaawansowanymi technologiami używanymi przez hakerów.

Najskuteczniejsza edukacja w zakresie cyberbezpieczeństwa to ta łącząca teorię z praktyką. Przykład ze strony Resilia to szkolenia interaktywne, które nie tylko informują o zagrożeniach, ale także angażują uczestników w realistyczne scenariusze, takie jak symulacje ataków phishingowych. Tego typu szkolenia pomagają pracownikom lepiej zrozumieć, jak wygląda potencjalne zagrożenie i jak na nie reagować. Kluczowe jest również stworzenie kultury bezpieczeństwa





w firmie, gdzie każdy pracownik czuje się odpowiedzialny za ochronę danych i systemów. Firmy, które regularnie komunikują swoim pracownikom wagę cyberbezpieczeństwa i włączają ich w procesy ochrony (np. koncepcja powołania ambasadatorów cyberbezpieczeństwa), są lepiej przygotowane na odparcie potencjalnych ataków.

Aktualnie wzmacnianie cyberbezpieczeństwa nie jest już tylko wyborem, staje się wymogiem. Do czego zobowiązują dyrektywy NIS2 i DORA i jakich podmiotów dotyczą? Co się stanie, jeśli nie zostaną wdrożone?

BS: Dyrektywa NIS2 (Network and Information Systems Directive) oraz rozporządzenie DORA (Digital Operational Resilience Act) są kluczowymi regulacjami, które nakładają obowiązki w zakresie cyberbezpieczeństwa na szeroką gamę podmiotów w Unii Europejskiej. NIS2 rozszerza zakres poprzedniej dyrektywy NIS, zobowiązując do wdrożenia odpowiednich środków ochrony nie tylko operatorów usług kluczowych, takich jak energetyka czy transport, ale również m.in. firmy logistyczne, producentów żywności, chemikaliów, a także

dostawców usług cyfrowych. DORA koncentruje się na sektorze finansowym, zobowiązując instytucje finansowe i dostawców technologii do wdrażania procedur zapewniających operacyjną odporność na zakłócenia, w tym cyberataki. Firmy muszą wdrożyć systemy zarządzania ryzykiem IT, które pozwalają na monitorowanie i minimalizowanie ryzyka.

Brak zgodności z tymi regulacjami może skutkować nie tylko wysokimi karami, ale również utratą licencji na prowadzenie działalności, co w przypadku sektora finansowego może mieć katastrofalne skutki.

Kierując się tym, że SEKA od lat wspiera organizacje w bezpiecznym prowadzeniu działalności, włączamy do naszego portfolio usługi audytu cyberbezpieczeństwa i identyfikacji podatności technicznych, szkolenia z cyberzagrożeń i zapewnienie zgodności z NIS2 i DORA oraz specjalistyczne doradztwo. Na co mogą liczyć nasi klienci decydujący się na te usługi i jakie korzyści dzięki nim odniosą?

MM: Klienci decydujący się na usługi oferowane przez SEKA

i Resilia mogą liczyć na kompleksowe wsparcie w zakresie cyberbezpieczeństwa, które obejmuje zarówno techniczne, jak i edukacyjne aspekty ochrony. Audyt cyberbezpieczeństwa przeprowadzony przez specjalistów Resilia pozwala na dogłębną analizę stanu zabezpieczeń organizacji i identyfikację słabych punktów, które mogą stanowić potencjalne zagrożenie.

W ramach szkolenia pracownicy zdobywają nie tylko teoretyczną wiedzę, ale także praktyczne umiejętności, które pozwalają na identyfikację i reakcję na cyberzagrożenia. Organizacje, które regularnie szkolą swoich pracowników, doświadczają znacznie mniej incydentów związanych z bezpieczeństwem IT.

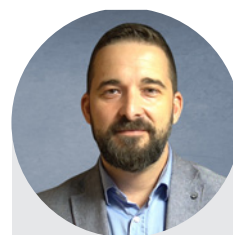
Wdrożenie zgodności z dyrektywą NIS2 i DORA to także kluczowy element oferty SEKA i Resilia. Dzięki temu firmy nie tylko spełniają wymogi prawne, ale również mogą działać zgodnie z najlepszymi praktykami w zakresie cyberbezpieczeństwa. Dodatkowo, dostęp do specjalistycznego doradztwa pozwala na opracowanie długoterminowej strategii, która zabezpiecza firmę przed nowymi zagrożeniami.

Jak Pana zdaniem będzie wyglądało cyberbezpieczeństwo za 5–10 lat? Jakie nowe wyzwania mogą się pojawić i jak firmy powinny już teraz się do nich przygotowywać?

BS: Cyberbezpieczeństwo za 5–10 lat będzie musiało sprostać zupełnie nowym wyzwaniom. Przewiduje się, że rozwój Internetu Rzeczy (IoT) spowoduje, że coraz więcej urządzeń będzie połączonych z siecią, co zwiększy powierzchnię ataku. Kolejnym istotnym aspektem będzie rozwój sztucznej inteligencji, która może być wykorzystywana zarówno przez atakujących, jak i obrońców.

AI może automatyzować ataki i uczynić je bardziej zaawansowanymi, ale także pozwoli na szybsze wykrywanie i neutralizowanie zagrożeń. Warto również zauważyć, że technologia blockchain może odegrać istotną rolę, zapewniając bardziej transparentne i bezpieczne transakcje.

Firmy już teraz powinny inwestować w badania i rozwój oraz w szkolenie swoich zespołów, aby być gotowości na te wyzwania. Ważne będzie także śledzenie najnowszych trendów technologicznych i legislacyjnych, oraz elastyczność w adaptacji do zmieniających się warunków. Długoterminowa strategia cyberbezpieczeństwa powinna uwzględniać różne scenariusze, aby firma była gotowa na każde zagrożenie. ■



Marcin Marczewski

CEO Resilia Sp. z o.o.



Bartosz Sadkowski

COO Resilia Sp. z o.o.,
Partner zarządzający
Crawford Polska Sp. z o.o.

Czy Twoi pracownicy zostali zaatakowani?

W realu takie pytanie może wydawać się dziwne, ale... nie w świecie cyfrowym. Badania pokazują, że nawet 90–95% naruszeń bezpieczeństwa w 2023 roku miało podłoże socjotechniczne, z czego większość była związana z phishingiem.

To znaczy, że codziennie Twoi pracownicy narażeni są na niebezpieczeństwo, jakim jest cyberatak z wykorzystaniem ich jako najsłabszego ogniwa.

MACIEJ MAZERANT
REDAKTOR PROWADZĄCY SEKA MAGAZYN



Phishing, czyli wyłudzenie informacji (w tym danych dostępowych do konta) za pomocą spreparowanych wiadomości e-mail czy sms, jest jednym z najpowszechniejszych sposobów ataku.

Przestępcy internetowi próbują oszukać Twojego pracownika i spowodować, aby dokonał czynności, które pozwolą dostać się do zasobów Twojej firmy. W tym celu mogą próbować nakłonić np. do instalacji **oprogramowania typu spyware**.

Fałszywe firmy kurierskie, urzędy administracji operatorzy telekomunikacyjni, czy nawet fałszywi koledzy z pracy starają się wyłudzić dane do logowania Twoich pracowników do systemów biznesowych, kont bankowych czy kont społecznościowych.

Wyjątkowo groźnym rodzajem phishingu, z którym będą musieli radzić sobie Twoi pracownicy, jest tzw. **spear-phishing**. Tego typu atak może skończyć się zainstalowaniem złośliwego **oprogramowania typu ransomware**, którego działanie unieruchomi sprzęt w całej organizacji. Konsekwencją będzie szantaż wymuszający okup w zamian za odblokowanie dostępu do danych i urządzeń. Aby uniknąć tragicznych w skutkach działań hakerów, należy wyposażać pracowników w niezbędną wiedzę i umiejętności, które zminimalizują ryzyko ataków.

Ważne jest również, aby tworzyć odpowiednie środowisko pracy, w którym zespół będzie miał czas na refleksję, związaną również z bezpieczeństwem w sieci. ■

Zobacz, na jakie cyberniebezpieczeństwa narażona jest Twoja firma:

- ataki DDoS
- podszywanie się pod DNS
- kradzież plików cookies
- ataki IoT
- clickjacking
- atak typu man-in-the-middle
- cross-site scripting
- ataki typu keylogger
- atak typu brute force
- atak słownikowy
- fałszywy WAP, czyli fałszywy bezprzewodowy punkt dostępu (Wireless Access Point)
- korzystanie z wycieków danych
- atak Bait and switch
- wstrzykiwanie kodu SQL
- blokada przeglądarki



Cyberbezpieczeństwo

Kompleksowa ochrona dla Twojej firmy w cyfrowym świecie



Zapewnij sobie spokój i stabilność biznesu. Nasz zespół ekspertów od cyberbezpieczeństwa zadba o Twoje cyfrowe zasoby, edukację pracowników oraz zapewnienie zgodności z aktualnymi przepisami w zakresie cyberbezpieczeństwa. Na każdym etapie współpracy zapewniamy niezbędne wsparcie i doradztwo.



Audyty
cyberbezpieczeństwa



Audyty podatności
technicznych



Wdrożenie zgodności
z NIS2 i DORA



Szkolenia
z cyberzagrożeń



Outsourcing usług
cyberbezpieczeństwa

Chcesz porozmawiać o cyberochronie dla swojej firmy?
Skontaktuj się z nami!

tel. 22 517 88 66

seka.pl

cyber@seka.pl

Rozwiązania skrojone na miarę

Zadowolony pracownik jest na wagę złota. Odpowiednia obsługa kadrowo-płacowa to ważna część tworzenia przyjaznego i budującego zaufanie zespołu środowiska pracy. Profesjonalnie zorganizowane procesy w tym obszarze pozwalają usprawnić funkcjonowanie firmy oraz zmniejszyć koszty jej utrzymania. O tym, dlaczego warto skorzystać z outsourcingu usług kadrowo-płacowych oraz szkolić pracowników działów kadr i płac, rozmawiamy z Elżbietą Zadrożną, Członkinią Zarządu ds. Finansowych SEKA, ekspertką z wieloletnim doświadczeniem w zakresie finansów i rachunkowości.

ELŻBIETA ZADROŻNA
CZŁONEK ZARZĄDU DS. FINANSOWYCH SEKA S.A.

W skrócie:

- Jakie są główne składowe usługi związanej z obsługą kadrowo-płacową?
- Kto najbardziej skorzysta z powierzenia obsługi kadrowo-płacowej firmie zewnętrznej?
- Na czym polegają szkolenia dla pracowników, którzy zajmują się kadrami i płacami w firmach?



Dla jakich organizacji przygotowana jest usługa out-sourcingu kadr i płac? Jakie wyzwania się z nią wiążą?

Naszą usługę kierujemy do małych, średnich i dużych firm. Wiemy, że każda firma jest wyjątkowa, dlatego stworzyliśmy rozwiązania naliczania płac i obsługi kadrowej właśnie po to, aby pomóc im w skoncentrowaniu się na statutowej działalności, a nie na naliczaniu płac i administracji kadrowej. Outsourcing kadrowo-płacowy pozwala usprawnić funkcjonowanie firmy oraz zmniejszyć koszty jej utrzymania. Doświadczenie specjalistów umożliwia uniknięcie błędów oraz skupienie się wyłącznie na właściwej działalności zamiast na dokumentacji. Firmy zyskują również komfort, gdy przeznaczony im specjalista zajmie się za nich kwestiami płac. Obsługujemy klientów o różnych profilach działalności na terenie całej Polski. Po podpisaniu umowy z każdym klientem opracowujemy szczegółowe zasady współpracy i harmonogramy przekazywania dokumentacji. Stale monitorujemy jakość obsługi i ogólną

satysfakcję klientów. Na podstawie uzyskanych wyników identyfikujemy obszary, które wymagają optymalizacji i wprowadzenia zmian.

Jako eksperci z wieloletnim doświadczeniem wiedz Państwo, co jest ważne w procesie obsługi kadrowo-płacowej. Czy właśnie w tym tkwi klucz do zapewnienia wyjątkowej kompleksowości obsługi?

Jakość usług kadrowo-płacowych to bardzo ważny element prawidłowo funkcjonującego przedsiębiorstwa. Obsługa kadrowa obejmuje bardzo złożony proces. W każdej firmie, w której są zatrudnieni pracownicy, istnieje potrzeba rozliczenia zatrudnienia. O ile w przypadku jednolitego zatrudnienia wszystkich pracowników w oparciu np. o umowę o pracę nie jest to tak złożone, to w przypadku różnych umów, zasad współpracy rodzi się szereg różnorodnych obowiązków. Pracownicy mają zróżnicowane nie tylko umowy ale również stawki opodatkowania, opcje ubezpieczenia; niektórzy pracownicy są rencistami, inni – na macierzyńskim urlopie, jeszcze

”

Jeżeli proces obsługi pracownika pod względem kadrowym i płacowym jest realizowany bez zastrzeżeń, to bezpośrednio wpływa to na zadowolenie zatrudnionych osób – może przekładać się na ich motywację do pracy oraz przywiązanie do pracodawcy.

Pamiętajmy, że zadowolony pracownik to wydajny pracownik.

inni – na zwolnieniu lekarskim. Obsługa kadrowo-płacowa polega przede wszystkim na właściwym obliczeniu wymiaru składek na ubezpieczenie zdrowotne, społeczne, wypadkowe oraz podatku, a ostatecznie również wynagrodzenia netto. Ponadto proces kadrowo-płacowy obejmuje także obliczenia premii, prowizji, wystawienie zaświadczeń dla pracowników, pasków miesięcznych, złożenie stosownych deklaracji urzędowych itd. Co więcej, w tym procesie mieści się również rozliczenie z pracownikami na wypowiadaniu, wypłata odpraw, nagród okolicznościowych itd. SEKA odpowiada w 100% za realizację tego procesu w sposób prawidłowy. W przypadku uchybień ponosimy odpowiedzialność materialną za poniesione przez klienta straty i zwracamy należność. Jeżeli proces obsługi pracownika pod względem kadrowym

i płacowym jest realizowany bez zastrzeżeń, to bezpośrednio wpływa to na zadowolenie zatrudnionych osób – może przekładać się na ich motywację do pracy oraz przywiązanie do pracodawcy. Pamiętajmy, że zadowolony pracownik to wydajny pracownik.

Jakie są główne składowe usługi związanej z obsługą kadrowo-płacową? Co klient dostaje w pakiecie i jaki jest model rozliczenia takiego wsparcia?

Zakres naszej usługi kadrowo-płacowej zależy od specyfiki firmy i jej indywidualnych potrzeb. Pewna część czynności jest jednak stała i niezależna od rodzaju działalności danej jednostki. Ogólnie można powiedzieć, że kompleksowo obsługujemy funkcjonowanie pracowników w przedsiębiorstwie.

Przykładowy zakres naszych czynności to:

- 1 przygotowywanie dokumentacji dotyczącej zatrudnienia pracownika, np. umowy o pracę, świadectwa pracy, zaświadczenia itd.;
- 2 prowadzenie, weryfikacja, przechowywanie i archiwizacja akt osobowych;
- 3 sporządzanie list płac i pozostałych dokumentów dotyczących ewidencji wynagrodzeń;
- 4 sporządzanie zestawień i analiz na potrzeby danej firmy;
- 5 rozliczenia z ZUS-em, urzędem skarbowym, PFRON-em, pracownicze plany kapitałowe, ubezpieczenia, benefity;
- 6 sporządzanie rocznych informacji o dochodach i składkach ZUS;
- 7 nadzór nad terminowością badań lekarskich i szkoleń BHP;
- 8 bieżące doradztwo w zakresie spraw pracowniczych.

Jak się zatem okazuje, zakres prac związanych z obsługą kadrowo-płacową jest bardzo szeroki. Co więcej, są to działania niezwykle ważne nie tylko dla funkcjonowania przedsiębiorstwa, ale przede wszystkim pracowników, którzy oczekują nieomyślności i przejrzystości w kwestii otrzymywanych wynagrodzeń, świadczeń socjalnych, świadczeń z zakresu ubezpieczeń zdrowotnych i społecznych itd.



Nasi klienci otrzymują w pakiecie możliwość kompleksowej obsługi w zakresie spraw pracowniczych. Każdą obsługiwaną firmę traktujemy indywidualnie – zarówno w kwestii obsługi, jak i rozliczeń. Analizujemy potrzeby klienta i staramy się dostosować naszą usługę tak, aby obie strony były zadowolone ze współpracy. Usługi wyceniamy w oparciu o liczbę zatrudnionych osób. Przedstawiana przez nas oferta cenowa zawiera koszt kompleksowej obsługi bez żadnych dodatkowych opłat. I myślę, że to właśnie wyróżnia naszą firmę.

Działają Państwo w pewnych ramach, przetestowanych schematach w oparciu o opracowane przypadki. Czy to pozwala na przewidywanie i „kreatywne” podejście do tak przecież różnorodnych problemów związanych z kadrami i płacami?

Oczywiście, musimy działać według ustalonych schematów. Tylko takie funkcjonowanie pozwala nam dbać o możliwie jak najlepszą jakość naszych usług. Kluczem do sukcesu jest

tu niewątpliwie doświadczony i zgrany zespół. Mamy również wsparcie merytoryczne w postaci zespołu prawników z zakresu prawa pracy. Do obsługi danego klienta staramy się odelegować pracownika, który już wcześniej miał doświadczenie w obszarze, w jakim klient prowadzi działalność. Pewne problemy często się bowiem powtarzają przy podobnej działalności i tym samym mając z nimi już wcześniej do czynienia, dysponujemy już wcześniej wypracowanymi rozwiązaniami.

Mnogość przepisów krajowych i europejskich, którym podlegają przedsiębiorcy, a także zawiłości prawne oraz rozwój technologiczny i społeczny powodują, że zarządzający firmami tracą energię na formalności, zamiast wykorzystywać ją do rozwoju organizacji. Czy usługa, którą Państwo świadczą, zdejmuje „ciężar” z barków przedsiębiorców, czy raczej oferuje wsparcie w jego dźwiganie?

Taki jest nasz główny cel działalności. Wspieramy przedsiębiorców w tym, co niezbędne



Wsparcie i bezpieczeństwo

Zlecając obsługę kadrowo-płacową na zewnątrz, pracodawca nie musi martwić się o znalezienie pracownika, bieżące przeszkolenie go, zapewnienie miejsca, sprzętu i oprogramowania do pracy w zakresie kadrowo-płacowym.

To duża oszczędność.

do funkcjonowania każdej jednostki, tak aby oni mogli skupić się na biznesie. Rzeczywiście zawitości prawne w zakresie prawa pracy i rozliczeń płacowych nadają sens naszej działalności. Zapewniamy naszym klientom przede wszystkim bezpieczeństwo w zakresie poprawności rozliczeń, ale też gwarantujemy ciągłość obsługi. Dla przykładu, w małej firmie zwykle sprawami kadr i płac zajmuje się jedna osoba. Wystarczy, że zachoruje lub skorzysta z dłuższego urlopu, a na ten czas nie ma jej kim zastąpić. U nas ciągłość wykonywania usługi musi być zapewniona. Nie bez znaczenia pozostaje również fakt, że zlecając obsługę kadrowo-płacową na zewnątrz, pracodawca nie musi martwić się o znalezienie pracownika, bieżące przeszkolenie go, zapewnienie miejsca, sprzętu i oprogramowania do pracy w zakresie kadrowo-płacowym. Myślę, że to duża oszczędność.

Oferują Państwo również szkolenia dla pracowników, którzy zajmują się kadrą i płacami w firmach. Czy to

znaczy, że dzielą się Państwo swoim wieloletnim doświadczeniem, dobrymi praktykami?

Na szkoleniach organizowanych przez SEKA wyrosło już kilka pokoleń kadrowców. Szkolimy w tym zakresie od prawie 30 lat. Nasi wykładowcy to przede wszystkim praktycy. Staramy się, aby uczestnicy naszych kursów zdobyli jak największą wiedzę i umiejętności zastosowania jej w pracy zawodowej. Dzielimy się z uczestnikami nie tylko wiedzą, ale i szerokim doświadczeniem w obszarze kadr i płac. Duża część zajęć to właśnie warsztaty. Prowadzący przedstawiają liczne przykłady ze swojego doświadczenia zawodowego, zapraszają uczestników do samodzielnego rozwiązywania zadań, które systematyzują i porządkują wiedzę oraz pomagają w zdobyciu praktyki z zakresu kadr i rozliczania wynagrodzeń. Dla nas jest to okazja do pozyskania pracowników do naszego działu outsourcingu kadrowo-płacowego.

Gdyby miała Pani przekonać przedsiębiorcę, że warto sko-

rzystać z usług kadrowo-płacowych, to jaki problem przedsiębiorstwa, który będzie rozwiązany dzięki tej współpracy, wskazałaby Pani jako pierwszy?

Jak już wspominałam, dostarczamy rozwiązania skrojone na miarę. Różne są powody, dla których firmy decydują się przekazać obsługę kadrowo-płacową na zewnątrz. W mniejszych firmach najczęściej decydują kwestie ekonomiczne, trudności z poprawnością rozliczeń i brak odpowiednich narzędzi informatycznych. W dużych firmach to najczęściej skomplikowanie tych rozliczeń, rozliczenie różnych systemów czasu pracy, obsługa zatrudnienia cudzoziemców, konieczność współpracy z zagraniczną centralą firmy itd. Zapewniam, że staramy się rozwiązać problem każdego klienta i właśnie to, że każdy problem traktujemy indywidualnie, niewątpliwie jest główną zachętą do podjęcia współpracy właśnie z naszą firmą.

Czy można powiedzieć, że za-

-płacową w SEKA, pozostaje nam tylko opłacić fakturę?

Tak, można tak powiedzieć. Oczywiście, oprócz naszej faktury klient musi jeszcze wypłacić wynagrodzenia, a także odprowadzić składki ZUS i podatki. Te przelewy jednak najczęściej, w zależności od nadanych nam uprawnień, przygotowujemy sami. Rzeczywiście można więc powiedzieć, że klientowi pozostaje w zakresie spraw pracowniczych opłacić naszą fakturę. ■



Elżbieta Zadrożna

Członek Zarządu
ds. Finansowych
SEKA S.A.

ESG – co trzeba o nim wiedzieć

Obowiązek wdrożenia wymogów zrównoważonego rozwoju i raportowania sprawia, że firmy będą musiały jeszcze uważniej przyglądać się temu, w jaki sposób wpływają na otoczenie i planują swoją strategię rozwoju. Jednak nowe wymagania nie przynoszą tylko nowych obowiązków dla firm. Ich spełnienie daje też wymierne korzyści. A to znaczy, że wiele może zależeć od tego, czy mamy w organizacji dobrze przygotowanego do swojej roli managera lub koordynatora ESG, który będzie odpowiedzialny za zbieranie, analizę i raportowanie danych, współpracę z otoczeniem biznesowym i szybkie reagowanie na zachodzące zmiany. O wszystkich najważniejszych kwestiach związanych z ESG rozmawiamy z Ewą Chodowską – ekspertką ESG, która jest mentorką nowego kursu SEKA „Manager ESG”.

EWA CHODOWSKA
EKSPERTKA ESG
MENTORKA NOWEGO KURSU SEKA „MANAGER ESG”

W skrócie:

- Co to takiego ESG?
- Jakie podmioty będą objęte nowymi obowiązkami?
- Jakich kompetencji oczekuje się od specjalistów ESG?
- Jaką ścieżkę kariery ma przed sobą manager ESG?

Skontaktuj się z nami
Dział Szkolenia
SEKA S.A.

tel.: 22 517 88 11
dzialszkolenia@seka.pl

”

Dokonanie wewnętrznej analizy własnej działalności pod kątem poszczególnych kryteriów ESG bardzo się przyda we współpracy z kontrahentami.



Zacznijmy od rozszyfrowania skrótu ESG. Co on oznacza?

ESG to skrót od angielskich słów: *environmental*, *social* (*responsibility*) i (*corporate*) *governance*. Uwzględnianie czynników ESG w zarządzaniu przedsiębiorstwem oznacza uwzględnianie wpływu, jaki wywiera ów podmiot na środowisko, społeczną odpowiedzialność i ład korporacyjny, oraz wzięcie pod uwagę wpływu tych czynników na funkcjonowanie danego przedsiębiorstwa. Mówiąc o ESG, często posługujemy się też pojęciem „zrównoważony rozwój”. To solidarność międzypokoleniowa, która polega na znajdowaniu takich rozwiązań gwarantujących dalszy wzrost, które pozwalają na aktywne włączenie w procesy rozwojowe wszystkich grup społecznych, dając im jednocześnie możliwość czerpania korzyści ze wzrostu gospodarczego.

Wcześniej był już CSR. Co nowego wnosi ESG?

W pewnym uproszczeniu można powiedzieć, że koncepcja ESG bazuje na idei CSR (*corporate*

social responsibility), czyli społecznej odpowiedzialności biznesu. CSR jednak kojarzony jest najczęściej z działaniami związanymi ze wzmacnianiem reputacji – w tym charytatywnymi – i rzeczywiście na ogół nie dotyczy podejmowania mierzalnych zobowiązań, a przynajmniej nie wynikały one z przepisów prawa bądź wyraźnych oczekiwań kontrahentów. Obecnie wymogi ESG wiążą się z podejmowaniem konkretnych zobowiązań oraz monitorowaniem i raportowaniem rezultatów działań podjętych przez organizację, a także weryfikacją stanu wdrożenia i przestrzegania wymagań w zakresie zrównoważonego rozwoju w naszym otoczeniu biznesowym.

Co daje firmom uwzględnianie czynników ESG w swojej działalności? Czy są to tylko korzyści wizerunkowe?

To znacznie więcej. Powiedziałbym, że to realna możliwość szczegółowej, dogłębnej analizy szans i ryzyk biznesowych – własnych oraz otoczenia biznesowego – konkurencji, kontrahentów, dostawców. Uwzględnienie ESG w działal-

ności przedsiębiorstwa pozwala na uzyskanie wiedzy o tym, w jaki sposób wpływamy na otoczenie w trzech wymiarach ESG, a zatem pozwala ocenić szanse – perspektywy biznesowe – oraz nawet potencjalne ryzyka dla naszego biznesu. Co więcej, pozwala uczynić to zarówno w krótko-, średnio-, jak i długoterminowym horyzoncie czasowym. Zintegrowanie czynników zrównoważonego rozwoju do działalności przedsiębiorstwa ma wpływ na jego wartość i pozycję konkurencyjną; przekłada się na jego pozycję finansową.

Jakie inne, bieżące korzyści oprócz wiedzy i możliwości analizy może uzyskać przedsiębiorstwo dzięki temu, że włączy czynniki ESG do swojej działalności, będzie je monitorować i raportować?

Niezależnie od tego, czy dane przedsiębiorstwo jest objęte obowiązkowym raportowaniem, może się okazać, że dokonanie wewnętrznej analizy własnej działalności pod kątem poszczególnych kryteriów ESG bardzo się przyda we współpracy z kontrahentami – zwłaszcza tymi, którzy

są zagranicznymi korporacjami czy podmiotami np. z rynku niemieckiego. Te podmioty już teraz przyjęły zobowiązania w zakresie badania spełnienia wymogów ESG u swoich kontrahentów – opracowały w tym celu szczegółowe, rozbudowane kwestionariusze, obejmujące szereg praktycznych pytań, w szczególności w aspektach środowiskowych i społecznych, takich jak relacje z pracownikami, zleceńodawcami, kontrahentami, dostawcami, społecznościami lokalnymi. Obserwujemy, że ESG jest swego rodzaju must-have nawet dla tych, którzy formalnie nie są objęci obowiązkiem raportowania.

Co to dokładnie znaczy?

Na przykład może się zdarzyć, że nasza oferta zostanie odrzucona w procesie przetargowym z uwagi na brak spełnienia wymogów związanych z ESG. Albo w toku istniejącej już ugruntowanej współpracy z kontrahentem zostaniemy poproszeni o dostarczenie informacji w zakresie ESG i brak ich dostarczenia może skutkować ograniczeniem lub zakończeniem współpracy. W wielu

Od kiedy firmy będą miały obowiązek raportowania?

Od 2024 r. – największe podmioty publiczne, spółki zatrudniające ponad 500 pracowników i spełniające kryteria finansowe, takie jak suma bilansowa powyżej 20 mln EUR i/lub roczne przychody powyżej 40 mln EUR. Pierwszy raport złożą w 2025 roku.

Od 2025 r. – duże spółki, które spełnią 2 z 3 kryteriów: zatrudnienie ponad 250 pracowników, suma bilansowa powyżej 25 mln EUR i/lub roczne przychody powyżej 50 mln EUR. Pierwszy raport złożą w 2026 roku.

Od 2026 r. – małe i średnie przedsiębiorstwa, które spełnią 2 z 3 kryteriów: zatrudnienie ponad 10 pracowników, suma bilansowa powyżej 350 tys. EUR i/lub roczne przychody powyżej 700 tys. EUR. Pierwszy raport złożą w 2027 roku.

Od 2027 r. – wybrane spółki z siedzibą poza UE mające w Polsce jednostkę zależną lub oddział, które osiągną na terenie UE roczne przychody powyżej 150 mln euro. Pierwszy raport złożą w 2028 roku.



finansowania oraz inwestycji. Z tego powodu dla wielu firm dobrej jakości raportowanie ESG będzie oznaczać lepszy dostęp do kapitału i niższy koszt jego pozyskania.

Jakie zmiany legislacyjne czekają nas w najbliższym czasie w aspekcie zrównoważonego rozwoju?

Możemy powiedzieć, że mamy do czynienia ze zmianami o charakterze przełomowym. Unijna dyrektywa w sprawie sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju (CSRD), opublikowana w grudniu 2022 r., ma zastosowanie do około 50 tys. spółek notowanych na giełdzie w UE lub prowadzących w Unii znaczącą działalność, niezależnie od miejsca siedziby.

CSRD nałoży na spółki obowiązek ujawniania obszernych, szczegółowych informacji na temat wyników w zakresie zrównoważonego rozwoju i powiązanych z nimi konsekwencji dla strategii biznesowej. Szczegółowe zasady ujawniania informacji zostały

określone w europejskich standardach sprawozdawczości w zakresie zrównoważonego rozwoju (ESRS).

Kolejnym krokiem milowym, który wywrze znaczący wpływ na działalność przedsiębiorstw, również tych nieobjętych wprost regulacją, jest dyrektywa CSDDD (Corporate Sustainable Due Diligence Directive) w sprawie należytej staranności w zakresie zrównoważonego rozwoju przedsiębiorstw. To akt prawny, który zobowiązuje duże przedsiębiorstwa działające na terenie Unii Europejskiej do identyfikacji, oceny i zarządzania negatywnym wpływem na środowisko i społeczeństwo. W praktyce ten obowiązek oceny obejmie także małe przedsiębiorstwa pozostające w relacjach biznesowych z dużymi kontrahentami. Aktualnie np. w Niemczech obowiązuje ustawodawstwo nakładające wymogi w zakresie należytej staranności na kontrahentów, co przekłada się na wiele firm polskich, dla których firmy niemieckie są partnerem eksportowym.

dużych przedsiębiorstwach wymogi ESG są już wpisane w umowy z dostawcami. Co więcej, dostawcy z określonych sektorów są zobowiązani do poddania się ocenie i przedstawienia odpowiednich certyfikatów, potwierdzających zgodność ich działalności z aktualnymi standardami ESG. A to jeszcze nie wszystko, bo kolejnym, istotnym aspektem związanym z ESG jest dostęp do finansowania i produktów finansowych.

W jaki sposób spełnienie wymogów ESG w przedsię-

biorstwie może mieć wpływ na finansowanie?

Patrząc na rynek europejski (i nie tylko), możemy dostrzec, że ustawodawca unijny nałożył szczególną rolę na instytucje finansowe w procesie tzw. zrównoważonej transformacji. Instytucje finansowe jako spółki giełdowe już od kilku lat są zobowiązane do raportowania zrównoważonego rozwoju i dodatkowo mają obowiązek monitorowania ryzyk ESG u swoich klientów oraz ujawniania wielu informacji związanych z przedmiotem udzielanego



Jakie podmioty będą objęte nowymi obowiązkami?

Nowymi obowiązkami zostaną objęte wszystkie spółki giełdowe notowane na rynku regulowanym w Unii Europejskiej, w tym MŚP (z wyjątkiem mikroprzedsiębiorstw). Warunkiem objęcia obowiązkiem raportowania jest spełnienie dwóch z trzech poniższych kryteriów:

- zatrudnienie ponad 250 pracowników;
- obrót netto przekraczający 40 mln EUR;
- bilans przekraczający 20 mln EUR.

W przypadku firm spoza UE działających w UE warunkiem obowiązkowego raportowania będzie spełnienie następujących kryteriów:

- obrót netto wygenerowany w UE przekraczający 150 mln EUR i spółka zależna w UE objęta zakresem CSRD

albo

- obrót netto wygenerowany w UE przekraczający 150 mln EUR i oddział w UE z rocznym obrotem netto

przekraczającym 40 mln EUR.

Natomiast spółki zależne będą zwolnione z obowiązku publikowania sprawozdań o zrównoważonym rozwoju, jeśli zostały uwzględnione w skonsolidowanym sprawozdaniu zarządu spółki dominującej, który został przygotowany zgodnie z wymogami CSRD, lub w skonsolidowanym sprawozdaniu o zrównoważonym rozwoju spółki dominującej z państwa trzeciego przygotowanym zgodnie z ESRS lub innym standardem uznanym za równoważny.

Czy przepisy dyrektywy CSRD to tylko zmiana sposobu raportowania?

To zdecydowanie coś więcej. Przepisy CSRD zobowiązują do wykazania, w jaki sposób firma oceniła możliwości i ryzyko biznesowe związane z kwestiami zrównoważonego rozwoju (w tym oddziaływania spółek na środowisko i społeczeństwo), a także możliwy wpływ na wyniki finansowe. Osoby zarządzające spółkami muszą wyjaśnić, czy i w jaki spo-



Warto wiedzieć!

ESG
Environmental,
Social, Governance

CSRD – Corporate
Sustainability
Reporting Directive

ESRS – European
Sustainability
Reporting
Standards

CSDDD
Corporate
Sustainable Due
Diligence Directive

sób ogólna strategia firmy uwzględni czynniki zrównoważonego rozwoju i ich konsekwencje finansowe, a także w jaki sposób planuje poprawić wyniki w zakresie zrównoważonego rozwoju.

Ze względu na nowe obowiązki firmy potrzebują specjalistów oraz managerów ESG.

Tak, wielość oraz różnorodny charakter wymogów ESG sprawia, że niezbędne staje się powołanie osoby, która zaprojektuje procesy związane ze zbieraniem i analizą danych, skoordynuje związane z tym czynności, w tym relacje z otoczeniem biznesowym, oraz na bieżąco będzie uważnie śledzić zmiany w tym kontekście.

Jakich kompetencji oczekuje się od specjalistów ESG?

Od osoby realizującej zadania z tego zakresu oczekuje się różnorodnych kompetencji z kilku obszarów – zarówno twardych, jak i miękkich, niezależnie od jej pozycji w strukturach danej organizacji. Określiłabym taką

Kurs „Manager ESG” w SEKA S.A.

Kurs przygotowuje do pełnienia roli managera ESG w organizacji.

Adresaci kursu:

- osoby chcące się przekwalifikować i zdobyć nowy zawód – managera ESG
- osoby wyznaczone przez organizację do pełnienia roli managera ESG

Korzyści:

- zdobycie niezbędnej wiedzy i umiejętności potrzebnych do pracy na stanowisku managera ESG
- praktyczne przygotowanie do pozyskiwania odpowiednich informacji i zebrania dokumentacji
- szerokie spektrum tematów związanych z ESG
- prowadzący to praktycy z doświadczeniem w obszarze ESG
- kurs w formie online

Sprawdź terminy
i program kursu
Zeskanuj kod QR



osobę jako multiinstrumentalistę. Niewątpliwie istotne są umiejętności analityczne – zarówno specjaliści, jak i managerowie ESG pracują z danymi z wielu obszarów działalności przedsiębiorstwa oraz jego otoczenia biznesowego, regulacje zaś nierzadko zawierają szereg wymogów jakościowych i ilościowych. Mówiąc o regulacjach, musimy mieć na uwadze umiejętność analizy aktów prawnych oraz standardów biznesowych, opracowań branżowych.

Które z tych kompetencji wskazałaby Pani jako kluczowe dla osiągnięcia sukcesu we wdrożeniu i bieżącej realizacji wymagań ESG?

Kluczowe w mojej opinii są kompetencje w zakresie komunikacji oraz budowania i utrzymywania relacji. Sukces zależy przede wszystkim



Kluczowe kompetencje managera ESG

Kompetencje w zakresie analizy danych, komunikacji oraz budowania i utrzymywania relacji. Sukces zależy od efektywnej współpracy w ramach całej organizacji.

od efektywnej współpracy w ramach całej organizacji. A skoro mówimy o komunikacji, to warto podkreślić, że przydatna będzie umiejętność precyzyjnego, zrozumiałego formułowania myśli – tworzenia dobrej jakości komunikacji dla różnorodnej grupy odbiorców.

Ekspert czy manager ESG to osoba, która potrafi przystępnym językiem mówić lub pisać o bardzo złożonych zagadnieniach, a nierzadko o nietatwych w odbiorze zmianach. Z uwagi na wspomnianą różnorodność aspektów zrównoważonego rozwoju konieczna jest otwartość i umiejętność szybkiego reagowania na zmiany.

Aby działać skutecznie, istotny jest więc miks umiejętności analitycznych, komunikacyjnych i relacyjnych. Kto w takim razie może zostać specjalistą lub managerem ESG? Czy

wykształcenie kierunkowe ma tu znaczenie?

Sam profil wykształcenia nie przesądza o sukcesie w tej dziedzinie. W większych podmiotach oczywiście tworzone są zespoły interdyscyplinarne. Jako specjalista lub manager ESG może sprawdzić się zarówno absolwent kierunków ścisłych, w tym nauk przyrodniczych, jak i humanista.

Czy możemy mówić obecnie o typowej ścieżce kariery dla specjalisty lub managera zrównoważonego rozwoju?

Można zaobserwować, że dość częstym zjawiskiem jest przechodzenie pracowników dotychczas zaangażowanych w firmie w kwestie PR, komunikacji marketingowej czy CSR do nowo powstających działów ESG. Z pewnością znajomość danej organizacji – specyfiki



Odpowiedź na praktyczne potrzeby

Do stworzenia naszego kursu zaangażowaliśmy praktyków – osoby, które od lat współpracują z klientami reprezentującymi różnorodne sektory działalności.

Naszym podstawowym założeniem jest zaprezentowanie praktycznych aspektów wdrożenia ESG i możliwych do osiągnięcia korzyści w związku ze zrównoważoną transformacją.

jej funkcjonowania, jej klientów, kontrahentów, procesów, osób zaangażowanych w poszczególne kwestie – ułatwia wdrażanie procesów ESG. Z tego powodu wiele firm w pierwszej kolejności poszukuje odpowiedniego kandydata wewnątrz własnej organizacji. Ponadto obserwujemy również migracje z innych podmiotów, a nawet sektorów. Kluczowe są kompetencje osobiste, gotowość na zmianę i chęć zaangażowania się w różnorodne wyzwania. Niezbędne jest jednak dostarczenie rzetelnych podstaw merytorycznych, a także możliwości wymiany wiedzy i doświadczeń. Takie możliwości chcieliśmy zaoferować naszym klientom, tworząc kurs. Wymagania są bardzo złożone i obszerne, a w dodatku ewoluują w sposób niezwykle dynamiczny, natomiast rynek często nie zdążył wypracować jednolitej praktyki. Przydatna

jest zatem możliwość wymiany refleksji lub wiedzy – w tej dziedzinie wszyscy są na etapie ciągłej nauki i doskonalenia swoich kompetencji, a na niektóre pytania może istnieć więcej niż jedna poprawna odpowiedź. Warto więc konfrontować swoje przemyślenia i wątpliwości z innymi ekspertami.

Biorąc pod uwagę duże wyzwania, jakie stoją przed osobami odpowiedzialnymi za raportowanie ESG, czym się kierowaliście, tworząc w SEKA kurs „Manager ESG”?

Trzeba podkreślić, że ESG jako dziedzina interdyscyplinarna wymaga szczególnego podejścia do edukacji. Aktualnie na rynku widzimy szeroką paletę szkoleń i studiów podyplomowych w tej dziedzinie. Uczelnie wyższe oferują liczne studia podyplomowe związane ze zrównoważonym rozwojem.

Naszym celem podczas opracowania koncepcji kursu była jak najlepsza odpowiedź na praktyczne potrzeby naszych klientów. Dlatego do jego tworzenia zaangażowaliśmy praktyków – osoby, które od lat współpracują z klientami reprezentującymi różnorodne sektory działalności. Naszym podstawowym założeniem jest zaprezentowanie praktycznych aspektów wdrożenia ESG i możliwych do osiągnięcia korzyści w związku ze zrównoważoną transformacją. Zależy nam na tym, by wskazywać na szanse i możliwości rozwiązań, by dzięki temu wyposażać naszych kursantów w różnorodne kompetencje, umożliwiając im samodzielne pełnienie tej fascynującej, przyszłościowej roli. ■



Ewa Chodowska

Mentorka kursu Manager ESG w SEKA S.A. Ekspertka ESG, prawniczka, menadżerka z wieloletnim doświadczeniem we wiodących kancelariach prawnych, globalnej firmie konsultingowej oraz bankowości. Posiada m.in. certyfikaty: Approved Compliance Officer (ACO) i Approved Compliance Expert (ACE). Aktywnie uczestniczy w projektach wdrożeniowych z zakresu ESG i stowarzyszeniach branżowych ESG.

Kaucja wraca

Jak wskazują badania, system kaucyjny na opakowania po napojach wpłynął bardzo pozytywnie na nawyki Europejczyków związane z segregacją wszystkich odpadów. To dobry prognostyk dla zmian w naszym kraju. Rozwój gospodarki o zamkniętym obiegu wiąże się z wyzwaniami i szansami, przed jakimi stoją wszyscy – producenci, przedstawiciele gmin i powiatów oraz konsumenci. Żeby nie zmarnować tych szans i sprostać wyzwaniom, powinniśmy być dobrze przygotowani do używania systemu kaucyjnego – zarówno pod względem merytorycznym, jak i logistycznym. Aby to ułatwić, przedstawiamy poradnik przygotowany przez Aleksandra Florka – Zastępcę Dyrektora Działu Handlowego ds. ochrony środowiska SEKA.

ALEKSANDER FLOREK
ZASTĘPCA DYREKTORA DZIAŁU HANDLOWEGO
DS. OCHRONY ŚRODOWISKA SEKA S.A.

W skrócie:

- Dlaczego ważne jest wprowadzenie systemu kaucyjnego?
- Jakiego typu przedsiębiorstwa są zobowiązane do wdrożenia systemu kaucyjnego w swojej działalności?
- Jak zmieni się życie zwykłych ludzi po wprowadzeniu przepisów kaucyjnych?



fot. Getty Images, Unsplash+

”

Wprowadzenie systemu kaucyjnego przyczynia się do ochrony środowiska, promuje edukację ekologiczną konsumentów, przynosi korzyści ekonomiczne i wspiera odpowiedzialność producentów.

Dlaczego ważne jest wprowadzenie systemu kaucyjnego? Komu to może się opłacać? A może nie o opłacalność tu chodzi?

Wprowadzenie systemu kaucyjnego jest ważne z kilku kluczowych powodów. Po pierwsze wpływa na ochronę środowiska poprzez między innymi:

- **redukcję odpadów**, ponieważ system kaucyjny motywuje konsumentów do zwracania opakowań, co zmniejsza ilość odpadów trafiających na składowiska;
- **recykling**, ponieważ zebrane opakowania mogą być mu poddawane, co zmniejsza zużycie surowców naturalnych i energii potrzebnej do produkcji nowych opakowań;
- **zmniejszenie zanieczyszczenia**, ponieważ ograniczenie liczby opakowań w środowisku przyczynia się do zmniejszenia zanieczyszczenia wód, gleby i powietrza.

Po drugie jest istotne z powodu ekonomicznego – opakowania zwrócone w ramach systemu kaucyjnego mają wyższą wartość jako surowce wtórne,

ponieważ są czystsze i łatwiejsze do segregacji. Firmy mogą zaoszczędzić na kosztach produkcji nowych opakowań, korzystając z materiałów z recyklingu.

Po trzecie system kaucyjny wzmacnia świadomość ekologiczną, edukując i motywując konsumentów do bardziej odpowiedzialnych zachowań w zakresie zarządzania odpadami. Regularne korzystanie z systemu kaucyjnego może prowadzić do trwałych zmian nawyków konsumenckich na korzyść bardziej ekologicznych wyborów.

Wdrożenie i obsługa systemu kaucyjnego wiąże się z potrzebą stworzenia nowych miejsc pracy w sektorze recyklingu i gospodarki odpadami. Dzięki mniejszej ilości odpadów gminy mogą zaoszczędzić, ponieważ zmniejszą koszty zarządzania odpadami.

Podsumowując, wprowadzenie systemu kaucyjnego przyczynia się do ochrony środowiska, promuje edukację ekologiczną konsumentów, przynosi korzyści ekonomiczne i wspiera odpowiedzialność producentów.

Jakiego typu przedsiębiorstwa są zobowiązane do wdrożenia systemu kaucyjnego w swojej działalności?

Do systemu kaucyjnego musi przystąpić każda jednostka handlu detalicznego – w tym m.in. punkty gastronomiczne, restauracje, kioski, stragany, bufety, punkty sprzedaży obwoźnej – lub hurtowego, sprzedająca napoje w opakowaniach objętych kaucją, tj.:

- jednorazowych butelkach z tworzyw sztucznych o pojemności do 3 l;
- wielorazowych butelkach szklanych o pojemności do 1,5 l;
- puszkach o pojemności do 1 l.

Ponadto ustawa dzieli jednostki handlu detalicznego i hurtowego, w których użytkownikom końcowym są oferowane napoje w opakowaniach objęte systemem kaucyjnym, na dwie grupy:

- jednostki o powierzchni sprzedaży nie większej niż 200 m²;
- jednostki o powierzchni sprzedaży powyżej 200 m².

Przedsiębiorca prowadzący jednostkę handlu detalicznego lub hurtowego o powierzchni sprzedaży nie większej niż 200 m², w której użytkownikom końcowym są oferowane produkty będące napojami w opakowaniach objętych systemem

kaucyjnym, jest obowiązany uczestniczyć w systemie kaucyjnym w zakresie co najmniej pobierania kaucji. Może również uczestniczyć w tym systemie w zakresie zwracania kaucji oraz zbierania pustych opakowań i odpadów opakowaniowych. Musi także zawrzeć umowę z co najmniej jednym podmiotem reprezentującym.

Przedsiębiorca prowadzący jednostkę handlu o powierzchni sprzedaży powyżej 200 m² jest obowiązany uczestniczyć w systemie kaucyjnym w pełnym zakresie, czyli pobierając i zwracając kaucje oraz zbierając puste opakowania i odpady opakowaniowe. Musi również zawrzeć umowę z każdym podmiotem reprezentującym.

Ustawa o gospodarce opakowaniami nie określa sposobu zbierania opakowań i odpadów opakowaniowych. Odbiór takich opakowań może nastąpić w kasach lub w specjalnie przygotowanych do tego miejscach na zasadzie zbiórki ręcznej. Możliwa też będzie zbiórka w tzw. butelkomatach, czyli automatach do zbiórki opakowań.

Przedsiębiorca objęty systemem kaucyjnym, który uczestniczy w nim w zakresie pobierania i zwracania kaucji oraz zbierania pustych opakowań i odpadów opakowaniowych,

fot. po lewej: Beatrice Mazzarello, Unsplash+



System kaucyjny może przyczynić się do wzrostu świadomości ekologicznej, motywując Polaków do bardziej odpowiedzialnego zarządzania odpadami, a tym samym do odpowiedniej ich segregacji.



będzie obowiązany do prowadzenia ewidencji w postaci papierowej albo elektronicznej. Ewidencja ta powinna obejmować:

- liczbę nabytych i sprzedanych produktów będących napojami w opakowaniach objętych systemem kaucyjnym;
- liczbę zwróconych opakowań i odpadów opakowaniowych;
- wysokość pobranych, zwróconych i niezwróconych kaucji.

W przypadku gdy prowadzący jednostkę handlową uczestniczyć będzie w systemie kaucyjnym jedynie w zakresie pobierania kaucji, będzie obowiązany do prowadzenia ewidencji w postaci papierowej albo elektronicznej, w danym roku kalendarzowym, obejmującej liczbę nabytych i sprzedanych produktów objętych systemem kaucyjnym. Ewidencję należy przechowywać przez 5 lat, licząc od pierwszego dnia roku kalendarzowego następującego po



Warto wiedzieć!

Osoba prowadząca jednostkę handlową uczestnicząca w systemie kaucyjnym jedynie w zakresie pobierania kaucji będzie obowiązana do prowadzenia ewidencji w postaci papierowej albo elektronicznej.

Ewidencję należy przechowywać przez 5 lat.

roku kalendarzowym, którego te informacje dotyczą. Warto podkreślić, że nie ma obowiązku składania sprawozdań sporządzanych na podstawie prowadzonej przez nich ewidencji.

Zgodnie z rozporządzeniem ministra klimatu i środowiska z dnia 8 lipca 2024 r. w sprawie wysokości kaucji dla poszczególnych rodzajów opakowań objętych systemem kaucyjnym wysokość kaucji za jedną sztukę opakowania wynosi:

- 0,50 zł w przypadku butelek jednorazowego użytku z tworzyw sztucznych o pojemności do trzech litrów, włącznie z ich zakrętkami i wieczkami z tworzyw sztucznych, z wyłączeniem szklanych lub metalowych butelek na napoje, których zakrętki i wieczka są wykonane z tworzyw sztucznych;
- 0,50 zł w przypadku puszek metalowych o pojemności do jednego litra;
- 1,00 zł w przypadku butelek szklanych wielokrotnego użytku o pojemności do półtora litra.

Czy system kaucyjny powinien zainteresować Kowalskiego/Kowską? Jak zmieni się życie zwykłych ludzi po wprowadzeniu tych przepisów? W lipcu 2019 r. 90% ankietowanych było przecież na TAK!

Wprowadzenie systemu kaucyjnego wpłynie na życie Polaka w kilku istotnych aspektach:

- podczas codziennych za-

kupów konsumenci będą musieli zapłacić kaucję za napoje w opakowaniach objętych systemem kaucyjnym. Choć kaucja będzie zwracana, może to wpłynąć na chwilowe zwiększenie kosztów zakupu. Konieczność zwracania butelek i puszek do sklepów lub punktów zbiórki będzie wymagać dodatkowego zaangażowania i organizacji ze strony konsumentów;

- system kaucyjny może przyczynić się do wzrostu świadomości ekologicznej, motywując Polaków do bardziej odpowiedzialnego zarządzania odpadami;
- Polacy będą bardziej zmotywowani do segregacji odpadów i dbania o to, aby zwracane opakowania były czyste i odpowiednio posegregowane. ■



Aleksander Florek

Zastępca Dyrektora
Działu Handlowego
ds. ochrony środowiska
SEKA S.A.



Ochrona środowiska

Kompleksowe wsparcie firm w realizacji obowiązków z zakresu ochrony środowiska



Miej pewność, że Twoja firma działa w zgodzie z prawem. Nasi eksperci zadbają o to w każdym aspekcie.



Audyty środowiskowe



Przygotowywanie KOBIZE, BDO, BDS i innych wymaganych wykazów i sprawozdań



Przygotowanie i odnawianie niezbędnych pozwoleń, rejestracji i zgłoszeń środowiskowych



Monitorowanie zmian prawnych



Reprezentowanie firmy podczas kontroli organów ochrony środowiska



Wdrażanie systemu zarządzania środowiskowego, zgodnie z normą PN-EN ISO 14001:2015 – Systemy zarządzania środowiskowego



Doradztwo w zakresie zarządzania emisją gazów cieplarnianych



Wyliczanie śladu węglowego

Potrzebujesz usług z zakresu ochrony środowiska? Skontaktuj się z nami!

seka.pl

srodowisko@seka.pl

Sprawniejsza praca

Pracownicy są przeciążeni obowiązkami i popełniają więcej błędów? Różne dane są rozproszone w firmie i trudno je znaleźć? Współpraca między zespołami od dawna szwankuje? Warto sprawdzić, jakie rozwiązania oparte na najnowszych technologiach pomogą usunąć te problemy. O tym, jak usprawnić codzienną pracę i podnieść jej efektywność, opowiada Ewa Klimczuk, General Manager z firmy Euvic, z którą SEKA współpracuje w zakresie wdrożonego nowego oprogramowania Microsoft 365.

EWA KLIMCZUK
GENERAL MANAGER, EUVIC

W skrócie:

- Czy digitalizacja w firmach jest konieczna?
- Jakie działy w firmie nie mogą się obyć bez digitalizacji?
- Które procesy w firmie najlepiej poddać robotyzacji i jakie wynikają z tego korzyści?
- Jak wygląda proces wdrażania AI do firmy?
- W jakich sytuacjach warto korzystać z outsourcingu IT?

EUVIC.

PARTNER SEKA S.A.

”

Firmy, które zwlekają z digitalizacją, nie mogą poprawić swojej efektywności operacyjnej, bo wciąż ponoszą zwiększone koszty działania, a to z kolei skutkuje utratą konkurencyjności na rynku.

Jak przebiega digitalizacja w polskich firmach? Co Państwo obserwują?

Digitalizacja w polskich firmach jest procesem dynamicznym i wielowarstwowym. Kluczowe trendy obejmują różne rozwiązania lub ich miks. Wśród najczęściej wdrażanych możemy wymienić elektroniczne obiegi dokumentów, które umożliwiają przechowywanie, śledzenie i zarządzanie dokumentami elektronicznymi w sposób zorganizowany i bezpieczny; RPA, czyli automatyzację obiegów dokumentów i procesów decyzyjnych, dzięki czemu przepływy pracy stają się szybsze i bardziej efektywne; a także przechowywanie danych w centralnych bazach danych lub systemach chmurowych, co ułatwia ich dostępność i integrację.

Organizacje decydują się też na integrację procesów. Polega ona na implementacji systemów ERP, które integrują różne funkcje back office, takie jak księgowość, zarządzanie zasobami ludzkimi, zarządzanie zapasami i zakupy, w jednej platformie. Takie rozwiązanie umożliwia centralizację danych i automatyzację procesów. Firmy wdrażają też systemy CRM, które pozwalają na lepszą obsługę klienta i personalizację oferty,

oraz systemy usprawniające pracę działów HR.

A jeśli chodzi o rozwiązania wspierające współpracę?

Zarządzając projektami, warto korzystać z narzędzi, które umożliwiają śledzenie postępów, zarządzanie zadaniami i współpracę zespołową. Z kolei platformy do współpracy online ułatwiają komunikację i koordynację pracy zespołowej.

Jakie mogą być konsekwencje tego, że wciąż odkładamy w czasie digitalizację procesów w firmie?

Konsekwencje odkładania digitalizacji sprowadzają się do dwóch podstawowych problemów, które cyfryzacja rozwiązuje. Przede wszystkim firmy, które zwlekają z digitalizacją, nie mogą poprawić swojej efektywności operacyjnej, bo wciąż ponoszą zwiększone koszty działania, a to z kolei skutkuje utratą konkurencyjności na rynku. Druga rzecz to problemy z jakością zarządzania. Brak cyfryzacji utrudnia poprawę jakości zarządzania, co może prowadzić do błędów i nieefektywności w działaniu firmy.

Jak zmienia funkcjonowanie firmy wprowadzenie digitalizacji procesów i które rozwiązania



pozwalają najszybciej zobaczyć plusy digitalizacji?

Wprowadzenie digitalizacji znacząco zmienia funkcjonowanie firmy poprzez usprawnienie i przyspieszenie procesów. Na przykład elektroniczny obieg dokumentów pozwala na szybszą obróbkę i lepszą organizację dokumentów, co przekłada się na efektywność operacyjną. Z kolei automatyzacja procesów decyzyjnych przyspiesza przepływ pracy i redukuje błędy. Na najszybsze efekty digitalizacji można liczyć przy wdrożeniu rozwiązań takich jak pełny elektroniczny obieg dokumentów oraz systemy zarządzania workflow. Platformy low-code wspierające zarządzanie również przynoszą szybkie rezultaty, umożliwiając łatwą integrację z istniejącymi systemami.

Jakie działy w firmie nie mogą się już obyć bez digitalizacji?

To na pewno administracja, która dzięki digitalizacji dokumentów i obiegowi informacji usprawniła

procesy administracyjne. Dużo zyskują na digitalizacji działy zarządzania zasobami ludzkimi, które mogą w ten sposób zautomatyzować powtarzalne procesy HR, takie jak rekrutacja, zarządzanie wynagrodzeniami czy ocena pracowników. Kolejny dział to obsługa klienta, który dzięki digitalizacji może ulepszyć zarządzanie danymi o klientach oraz obsługą zapytań.

Usprawnieniem może być również wprowadzenie robotyzacji procesów. Które procesy w firmie najlepiej poddać robotyzacji i jakie wynikają z tego korzyści?

Tu warto wskazać dwa procesy: wprowadzanie danych i wystawianie faktur – automatyzacja tych procesów redukuje błędy, oszczędza czas i przyspiesza operacje. A drugi to automatyzacja obsługi klienta. Zarządzanie reklamacjami i przetwarzanie zgłoszeń serwisowych poprawia jakość obsługi, przyspiesza odpowiedź i zmniejsza obciążenie pracowników.



Głośnym tematem jest wprowadzanie sztucznej inteligencji do procesów czy usług. Wiele badań wskazuje na to, że rozwiązania wykorzystujące AI mogą znacząco podnieść produktywność pracowników, a dzięki temu budować przewagę konkurencyjną. Na ile polskie firmy są otwarte na korzystanie z AI?

Obserwujemy, że polskie firmy są coraz bardziej otwarte na korzystanie z AI, dotyczy to szczególnie takich branż, jak: technologia, handel, bankowość, ubezpieczenia, logistyka itp. W tych sektorach potrzeba AI jest dobrze rozumiana jako narzędzie budowania przewagi konkurencyjnej.

Natomiast bardziej sceptyczne wobec AI są zazwyczaj te branże mniej zaawansowane technologicznie lub mające ograniczone zasoby na inwestycje w nowe technologie. To zwykle małe i średnie przedsiębiorstwa w tradycyjnych branżach czy branże o niższym poziomie cyfryzacji.

Założmy, że chcemy wprowadzić AI do naszej firmy. Jak wygląda proces jej wdrażania?

Proces wprowadzenia AI składa się z kilku etapów. Pierwszy to zbadanie, w których obszarach firmy można wprowadzić AI, na podstawie analizy danych i potrzeb. Kolejny etap to przygotowanie odpowiednich danych, które są niezbędne do wyuczenia modelu AI. Następnie przechodzimy do stworzenia rozwiązania prototypowego, które testuje możliwości AI w kontekście specyficznych potrzeb firmy. Rozwijamy rozwiązanie docelowe i wyuczamy model na danych klienta. Ostatni etap to regularne monitorowanie wyników i optymalizacja modelu zgodnie z potrzebami danej firmy.

Niektórzy jednak obawiają się stosowania sztucznej inteligencji. Wiąże się to z obawą o naruszenie praw autorskich, błędy, jakie popełnia AI. Czasem to strach, że sztuczna inteligencja odbierze nam pracę.



Warto wiedzieć

Polskie firmy są coraz bardziej otwarte na korzystanie z AI, dotyczy to szczególnie takich branż, jak: technologia, handel, bankowość, ubezpieczenia, logistyka itp. W tych sektorach potrzeba AI jest dobrze rozumiana jako narzędzie budowania przewagi konkurencyjnej.

Co Państwo odpowiadają na te obawy?

Jako firma zajmująca się wdrożeniami AI, możemy powiedzieć, jakie jest nasze podejście do tych kwestii, tak aby AI nie budziła obaw, a wzmacniała efektywność i bezpieczeństwo organizacji.

Jeśli chodzi o naruszenie praw autorskich, możemy zapewnić, że nasze rozwiązania AI są zgodne z przepisami prawa i normami etycznymi. Dbamy o to, aby dane wykorzystywane do trenowania modeli były pozyskane w sposób legalny, a prawa autorskie były respektowane. Regularnie monitorujemy zmiany w regulacjach prawnych, aby zapewnić pełną zgodność.

Zdajemy sobie sprawę, że AI nie jest wolna od błędów. Dlatego stosujemy rygorystyczne procedury testowania i walidacji naszych rozwiązań. Każde wdrożenie jest wspierane przez zespół ekspertów, który monito-



ruje działanie systemu i wprowadza niezbędne poprawki, aby zminimalizować ryzyko błędów.

Traktujemy AI jako narzędzie, które ma na celu wspieranie ludzi w pracy, a nie zastępowanie ich. Nasze rozwiązania projektujemy więc tak, aby zwiększyć efektywność pracy, a nie eliminować miejsca pracy. Wspieramy naszych klientów w przygotowywaniu pracowników do współpracy z AI, oferując szkolenia i wsparcie w adaptacji do nowych technologii.

Powiedzmy jeszcze, w jakich sytuacjach warto korzystać z outsourcingu IT? Co powinno być dla firmy sygnałem, że potrzebuje takiego rozwiązania?

Sygnały, że firma może potrzebować outsourcingu IT, to m.in. problemy z zarządzaniem infrastrukturą IT, rosnące koszty operacyjne, trudności w utrzymaniu i aktualizacji technologii oraz potrzeba dostępu do nowoczesnych narzędzi i ekspertów. Możemy więc wymienić

kilka sytuacji, kiedy outsourcing IT jest korzystnym rozwiązaniem.

Zacznijmy od tej, gdy firma nie dysponuje wystarczającym zespołem IT. Wówczas outsourcing pozwala na dostęp do wysoko wykwalifikowanych specjalistów i technologii, które są kosztowne w utrzymaniu na własną rękę. Outsourcing może być też bardzo opłacalny niż utrzymywanie wewnętrznego działu IT w przypadku małych i średnich firm. W sytuacji, gdy firmy realizują projekty wymagające zaawansowanej technologii lub specjalistycznej wiedzy, outsourcing umożliwia dostęp do ekspertów, które są trudne do znalezienia wewnątrz. I wreszcie outsourcing pozwala na elastyczne dostosowywanie zasobów IT do zmieniających się potrzeb firmy, co jest szczególnie ważne w dynamicznych branżach.

Które z tych powyższych rozwiązań stosują Państwo u siebie? I co możecie powiedzieć o własnych doświadczeniach z ich wdrożeniem?

Outsourcing IT

Sygnały, że firma może potrzebować outsourcingu IT, to m.in.

- 1 problemy z zarządzaniem infrastrukturą IT,
- 2 rosnące koszty operacyjne,
- 3 trudności w utrzymaniu i aktualizacji technologii,
- 4 potrzeba dostępu do nowoczesnych narzędzi i ekspertów.

Outsourcing pozwala na elastyczne dostosowywanie zasobów IT do zmieniających się potrzeb firmy, co jest szczególnie ważne w dynamicznych branżach.

W naszej firmie stosujemy wiele opisanych wcześniej rozwiązań. Wdrożyliśmy m.in. systemy do zarządzania dokumentami, co ułatwiło nam organizację pracy i zwiększyło bezpieczeństwo danych. Używamy narzędzi do automatyzacji obiegu dokumentów oraz zarządzania projektami, co przyczyniło się do zwiększenia efektywności i lepszej koordynacji w zespole. Korzystamy z systemów ERP. Testujemy też i wdrażamy rozwiązania AI w różnych obszarach, aby zwiększyć naszą efektywność i innowacyjność. Nasze doświadczenia pokazują, że AI przynosi wymierne korzyści, ale wymaga starannego planowania i monitorowania.

Wdrażanie tych rozwiązań wiązało się z początkowymi

wyzwaniami, takimi jak adaptacja zespołu i integracja z istniejącymi systemami, jednak długofalowo przyniosło znaczne usprawnienia i korzyści w codziennej działalności. ■



Ewa Klimczuk

General Manager
Euvic

Ciągle się pali!

Co robić z ochroną przeciwpożarową w moim zakładzie pracy?

W tym roku nie ma chyba miesiąca bez informacji o dużym pożarze. Z ogniem zmagano się zarówno w miastach wojewódzkich, jak i w znacznie mniejszych miejscowościach na terenie całego kraju. W walce z żywiołem uczestniczyły setki strażaków. Pożary niosą zagrożenie dla życia i generują ogromne straty. Obecnie budzą jeszcze dodatkowy niepokój, że mogą być nieprzypadkowe, ze względu na sytuację za naszą wschodnią granicą. Przyczyny pożarów ustalą biegli. Natomiast wszyscy odpowiedzialni za ochronę przeciwpożarową zakładów pracy i obiektów użyteczności publicznej powinni jeszcze bardziej upewnić się, że niczego nie zaniedbano w tej kwestii i zrobiono wszystko, by zapewnić bezpieczeństwo. O tym, jak sprawdzać zgodność ochrony przeciwpożarowej z obowiązującymi wymogami, pisze dr inż. Jan Kołdej, koordynator ds. nadzoru PPOŻ. SEKA S.A.

DR INŻ. JAN KOŁDEJ
KOORDYNATOR DS. NADZORU PPOŻ.
SEKA S.A.

W skrócie:

- Czarna seria pożarów w Polsce?
- Jakie są najczęstsze przyczyny pożarów?
- Audyt PPOŻ., czyli audyt stanu bezpieczeństwa pożarowego zakładu pracy.
- Co sprawdzamy podczas audytu PPOŻ.?

”

Zgodnie z ustawą o ochronie przeciwpożarowej, obowiązek dbania o bezpieczeństwo pożarowe spoczywa na właścicielu, użytkowniku bądź zarządcy budynku.



Pożar Centrum Marywilska 44
fot. sekc. Krzysztof Pisz, Wydział Prasowy KG PSP

Czarna seria pożarów w Polsce?

W pierwszym i drugim kwartale bieżącego roku doszło w Polsce w krótkim odstępie czasu do kilkunastu bardzo dużych pożarów pod względem ich kubatury i powierzchni, ale także ze względu na skutki finansowe oraz środowiskowe dla lokalnego społeczeństwa.

Najszerzym echem odbił się pożar Centrum Marywilska 44 w Warszawie. Doszło do niego w godzinach porannych w niedzielę 12 maja 2024 r. Ogniem objęte zostało ponad 80 proc. hali o wymiarach 250 x 250 m. W rezultacie przestrzeń, w której mieściło się około 1400 stoisk sprzedażowych, niemalże doszczętnie spłonęła w błyskawicznym tempie rozprzestrzeniania się pożaru.

Ale palić zaczęło się już wcześniej i na Marywilskiej się niestety nie skończyło. Przypomnijmy pożary chronologicznie od początku roku, sięgając do publikacji Komendy Głównej Państwowej Straży Pożarnej.

3 marca 2024 r. w godzinach wczesnoporannych, w miejscowości Kanin na Pomorzu doszło do pożaru czterech hal produkcyjnych o łącznej powierzchni ok. 4500 m².

1 kwietnia 2024 r. w Tychach doszło do wybuchu gazu w budynku wielorodzinnym. W wyniku zdarzenia uszkodzanych zostało 13 osób. Spośród nich siedem osób, w tym dwoje dzieci, zostało przewiezionych do szpitala. Ewakuowano wszystkich mieszkańców budynku.

9 kwietnia 2024 r. doszło do pożaru hali produkcyjnej w Mikołowie. W wyniku zdarzenia nikt nie ucierpiał. Objęty ogniem budynek stanowił część kompleksu bezpośrednio połączonych ze sobą budynków. Powierzchnia pożaru to ponad 3200 m².

10 maja 2024 r. wybuchł pożar na składowisku odpadów w Siemianowicach Śląskich o powierzchni ok. 6000 m². W kulminacyjnym momencie w działania zaangażowanych było ponad 230 strażaków oraz 90 samochodów.

W nocy **12/13 maja 2024 r.** doszło do pożaru w zajezdni autobusowej w Bytomiu. Spłonęło 10 autobusów, a osiem zostało uszkodzonych.

1 lipca 2024 r. w godzinach popołudniowych w miejscowości Wola Łaska w województwie łódzkim na terenie firmy zajmującej się recyklingiem doszło do pożaru hałdy odpadów o powierzchni ok. 4000 m² oraz zlokalizowanej w pobliżu hali o powierzchni 800 m². W gaszeniu pożaru uczestniczyło łącznie ok. 160 strażaków. W zdarzeniu zostało uszkodzonych 11 osób.

10 lipca 2024 r. w godzinach przedpołudniowych wybuchł pożar w części magazynowej marketu budowlanego w Krośnie. Przed przyjazdem straży pożarnej ze sklepu ewakuowało się 40 osób; nikt nie został ranny. W gaszeniu trwającego wiele godzin pożaru łącznie uczestniczyło ponad 300 strażaków.

W nocy **12/13 lipca 2024 r.** w miejscowości Malec wybuchł pożar w fabryce produkującej Paluszki Beskidzkie. Nikt nie zo-

stał uszkodzony, ale ogień objął dwie z trzech hal produkcyjnych. Dach jednej z nich całkowicie się zawalił, a dach drugiej – częściowo.

14 lipca 2024 r. przed godz. 17.00 do stanowiska kierowania Komendy Miejskiej PSP w Gdańsku wpłynęła informacja o pożarze hali magazynowej w porcie Gdańsk. W wyniku pożaru zawaleniu uległ częściowo dach hali. Łączna powierzchnia pożaru – 6500 m². Uratowano drugą część hali oraz budynek sąsiadujący z pomieszczeniami biurowymi.

Przyczyny ostatnich pożarów pod lupą służb państwowych

Przyczyny tych wszystkich pożarów będą wyjaśniane przez policję oraz biegłych z zakresu pożarnictwa. Mimo że w przypadku niektórych ostatnich dużych pożarów na terenie naszego kraju już na tym etapie postępowania wykluczono celowe podpalenie, to każdy z nich budzi podejrzenia o potencjalną działalność dywersyjną inspirowaną przez



Pożar w Porcie Gdańsk
fot. mł. asp. Łukasz Rutkowski, PSP



Pożar hal w Kaninie
fot. strona KG PSP

Jakie są najczęstsze uchybienia w ochronie przeciwpożarowej?

W trakcie realizowania audytu najczęściej są stwierdzane:

- uchybienia dotyczące wymaganej w obiekcie dokumentacji (w tym aktualność Instrukcji Bezpieczeństwa Pożarowego),
- niezgodności w bieżącej eksploatacji podstawowego sprzętu gaśniczego i instalacji przeciwpożarowych.

obce służby. Niektóre z nich mówiły nawet o potencjalnym sabotażu. Takiego scenariusza nie wykluczają również osoby odpowiadające za bezpieczeństwo Polski. W tym gronie jest między innymi szef Biura Bezpieczeństwa Narodowego Jacek Siewiera czy minister MSWiA Tomasz Siemoniak, który w lipcu br. mówił w wywiadzie dla jednej ze stacji informacyjnych, że „każdy, zwłaszcza bardziej spektakularny pożar, jest analizowany przez ABW. Jest tu ustanowiona ścisła współpraca Państwowej Straży Pożarnej, Policji i ABW”. Siemoniak mówił również: „Doświadczenia ostatnich miesięcy pokazują,

że w każdej sytuacji trzeba brać pod uwagę działanie obcej agentury, która zleca jednemu z agentów podpalenie różnych obiektów”.

Najczęstsze przyczyny pożarów

Biorąc pod uwagę obecną sytuację w naszym obszarze geopolitycznym, działalność dywersyjna jest oczywiście możliwa. Jednak na podstawie wielu postępowań w sprawie przyczyn powstania pożarów można przyjąć, że występują przede wszystkim takie główne czynniki, jak:

- zaniedbania w stosowaniu obowiązujących przepisów dotyczących ochrony PPOŻ., instrukcji i regulaminów dotyczących przebiegu procesu technologicznego czy innych czynności stosowanych w zakładzie,
- sam przebieg procesu technologicznego oraz innych czynności realizowanych w zakładzie,
- brak właściwego nadzoru pracodawcy nad realizacją obowiązujących ustaleń przez pracowników.

- charakteru ich działalności;
- rodzaju produkcji, usługi;
- technologii;
- wielkości;
- innych specyficznych czynników.

Poziom zagrożenia życia ludzi w budynkach mieszkalnych, biurowych czy obiektach przemysłowych podczas pożaru zależy zdecydowanie od takich kwestii, jak:

- stan przepisów techniczno-budowlanych i przeciwpożarowych, regulujących kwestie projektowania, budowy i eksploatacji budynków;
- stopień przestrzegania tych przepisów przez wszystkich, których one dotyczą;
- możliwość skutecznego i efektywnego prowadzenia akcji ratowniczej przez jednostki ochrony przeciwpożarowej;
- nasze zachowanie – czy damy sobie szansę na przeżycie?

Zgodnie z Ustawą z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2009 r. nr 178, poz. 1380 z późn. zm.) art. 4.1. właściciel, zarządca lub użytkownik budynku, obiektu lub terenu, zapewniając jego ochronę przeciwpożarową, obowiązany jest w szczególności:

Organizacja ochrony przeciwpożarowej w zakładzie pracy

Pod pojęciem zorganizowania systemu ochrony przeciwpożarowej w zakładzie pracy należy rozumieć dwa podstawowe aspekty bezpieczeństwa z tego zakresu, to jest:

- powszechność stosowania obowiązujących przepisów, zasad postępowania zgodnie z instrukcjami, nakazami i przyjętymi ustaleniami;
- właściwy nadzór nad realizacją obowiązujących ustaleń.

Organizacja ochrony przeciwpożarowej w zakładach pracy jest różna i uzależniona od:



Pożar na składowisku odpadów w Siemianowicach Śląskich
fot. kpt. Mateusz Krzystański, PSP



Wybuch gazu w budynku wielorodzinnym
fot. strona KG PSP

- przestrzegać przeciwpożarowych wymagań budowlanych, instalacyjnych i technologicznych;
- zapewnić konserwację i naprawy sprzętu oraz urządzeń określonych w pkt. 2, zgodnie z zasadami i wymaganiami gwarantującymi sprawne i niezawodne ich funkcjonowanie;
- zapewnić osobom przebywającym w budynku, obiekcie lub na terenie bezpieczeństwa i możliwość ewakuacji;
- przygotować budynek, obiekt lub teren do prowadzenia akcji ratowniczej;
- zaznajomić pracowników z przepisami przeciwpożarowymi;
- ustalić sposoby postępowania na wypadek powstania pożaru, klęski żywiołowej lub innego miejscowego zagrożenia.

Audyt PPOŻ., czyli audyt stanu bezpieczeństwa pożarowego zakładu pracy

Polskie prawo dokładnie określa sposoby i warunki ochrony przeciwpożarowej w budynkach. Ich zarządcy są zobowiązani do realizacji obo-



Co sprawdzamy podczas audytu PPOŻ.?

Analizie poddawane są:

1

Urządzenia przeciwpożarowe i gaśnice

2

Drogi ewakuacyjne

3

Przygotowanie do przeprowadzenia ewentualnej akcji ratowniczej (w tym drogi pożarowe)

wiązujących przepisów, a za ich nieprzestrzeganie grożą sankcje karne. Wiedząc, jak ważne są to kwestie, warto poddawać zewnętrznej ocenie wszystkie wdrożone działania mające zapewnić ochronę przeciwpożarową. Jak to zrobić? Audyt PPOŻ. to najlepszy sposób na sprawdzenie, czy wszystkie wymogi prawne zostały spełnione oraz czy w razie pożaru ewakuacja osób zagrożonych jest możliwa.

Audyt PPOŻ. odpowiada za sprawdzenie wszystkich wymagań pod względem ochrony przeciwpożarowej, przewidzianych w danym obiekcie. Uwzględnia analizę stanu bezpieczeństwa przeciwpożarowego w budynku, tj.: wyposażenie w sprzęt i instalacje przeciwpożarowe, warunki ewakuacji oraz możliwość prowadzenia akcji ratowniczo-gaśniczej.

Jak przeprowadzamy audyt z zakresu PPOŻ. w SEKA?

SEKA wspiera firmy w bezpiecznym prowadzeniu biznesu oraz instytucje w bezpiecznym prowadzeniu działalności, dlatego wśród naszych usług nie mogło zabraknąć audytów PPOŻ. Przeprowadzamy je od wielu lat. Mamy ogromne

doświadczenie oraz wykwalifikowaną kadrę specjalistów.

Jak wygląda nasze podejście do audytu PPOŻ.? Przeprowadzając audyt z zakresu bezpieczeństwa przeciwpożarowego, przede wszystkim sprawdzamy, czy budynek jest pod tym względem bezpieczny. Wskazujemy ewentualne uchybienia oraz sprawdzamy, czy wszystkie obowiązki zostały dopełnione i zrealizowane, aby uniknąć potencjalnych kar czy poważniejszych konsekwencji w przypadku wybuchu pożaru.

Audyt PPOŻ. może stanowić część audytu BHP lub może być wykonany oddzielnie. Nawet jeśli właściciel budynku zatrudnia osoby odpowiedzialne za bezpieczeństwo przeciwpożarowe, warto od czasu do czasu przeprowadzić niezależny audyt. Nasza rekomendacja to audyt co najmniej raz na 5 lat lub częściej, jeśli doszło do istotnych zmian w funkcjonowaniu zakładu.

Co sprawdzamy podczas audytu PPOŻ.?

Obejmuje on wszystkie poniższe czynności:

- weryfikacja wyposażenia budynków w sprzęt i instalacje przeciwpożarowe;



Jak postępować w sytuacji, gdy audyt PPOŻ. wykaże niezgodności w obiekcie?

W takim wypadku w dokumencie zawierane są dodatkowe informacje m.in. o tym, jak doprowadzić budynek do stanu, który jest zgodny z przepisami. Możemy również zaoferować sporządzenie stosownej dokumentacji oraz przeprowadzanie bieżących konserwacji i przeglądów podstawowego sprzętu gaśniczego i instalacji PPOŻ.

Pożar hali w Mikołowie
fot. ogn. Dawid Strączek, Państwowa Straż Pożarna

- sprawdzenie stanu przestrzegania obowiązujących przepisów;
- weryfikacja poprawności dokumentacji przeciwpożarowej, czyli poprawności wykonania i aktualizacji Instrukcji Bezpieczeństwa Pożarowego;
- ocena obowiązujących procedur na wypadek zaistnienia pożaru lub innego miejscowego zagrożenia;
- przegląd warunków ewakuacji w budynku;
- audyt z zakresu bezpieczeństwa wybuchowego, tj. określenie pomieszczeń i stref zagrożonych wybuchem;
- kontrola regularności praktycznego sprawdzenia organizacji oraz warunków ewakuacji z całego obiektu;
- weryfikacja poprawności i aktualności przeprowadzonych szkoleń z zakresu bezpieczeństwa PPOŻ.;
- kompleksowy raport finalizujący przeprowadzony audyt PPOŻ.

Audyt PPOŻ stanowi gwarancję bezpieczeństwa i spełnienia wszystkich obowiązujących aktualnie przepisów. Warto

podkreślić, że nasze doświadczenie obejmuje przeprowadzanie audytów w budynkach o różnej specyfice, pełniących specyficzne funkcje – magazynowe, produkcyjne, biurowe, handlowe, mieszkaniowe – co wiąże się z różnorodnymi zagrożeniami pożarowymi lub wybuchowymi. Nasi audytorzy doskonale znają specyfikę swojej pracy, a dodatkowo współpracujemy z cenionymi branżowymi ekspertami i rzeczoznawcami PPOŻ., dzięki czemu możemy kompleksowo zadbać o bezpieczeństwo przeciwpożarowe.

Podsumowując, audyt z zakresu ochrony przeciwpożarowej umożliwia zweryfikowanie wszystkich nieprawidłowości bez konsekwencji prawnych. Pozwala również usunąć wszelkie niezgodności i uniknąć ewentualnych konsekwencji wyciąganych przez uprawnione organy kontroli.

Kto szczególnie powinien rozważyć audyt PPOŻ.?

Mając na uwadze aktualną sytuację – czyli fakt, że jeste-



Warto wiedzieć!

Audyt z zakresu ochrony przeciwpożarowej umożliwia zweryfikowanie i usunięcie wszystkich nieprawidłowości bez konsekwencji prawnych.

Nasza rekomendacja to **audyt co najmniej raz na 5 lat lub częściej**, jeśli doszło do istotnych zmian w funkcjonowaniu zakładu.

śmy krajem przyfrontowym, w którym mogą się zdarzać akty dywersji i sabotażu – oraz mając w pamięci pożary, do jakich dochodziło w ostatnich miesiącach i ich specyfikę, o audycie PPOŻ. szczególnie powinni pomyśleć właściciele/zarządcy wielkich i średnich magazynów, hal targowych, produkcyjnych, a także składowisk odpadów, wszelkich powierzchni biurowych, placówek oświatowych i innych obiektów użyteczności publicznej. ■



dr inż.
Jan Kołdej

Koordinator
ds. nadzoru PPOŻ.
SEKA S.A.



Audyt PPOŻ.

Kompleksowa ocena stanu
budynku pod kątem
pożaru i ewakuacji



Nie ryzykuj, zadbaj o bezpieczeństwo! Sprawdź, czy Twój budynek jest dobrze zabezpieczony na wypadek pożaru i przygotowany do ewakuacji. Audyt PPOŻ. to gwarancja bezpieczeństwa i spełnienia wszystkich obowiązujących aktualnie przepisów.

Podczas audytu sprawdzamy:

- Poprawność i aktualność przeprowadzonych szkoleń ppoż.
- Wyposażenie budynku w sprzęt i instalacje ppoż.
- Poprawność procedur i dokumentacji ppoż.
- Przestrzeganie obowiązujących przepisów
- Stopień zagrożenia wybuchem
- Warunki ewakuacji

Audyt kończy szczegółowy raport wraz z rekomendacjami zmian, jakie należy wprowadzić, by spełniać wszystkie wymogi prawne.

Dlaczego warto nam zaufać?

- Współpraca z branżowymi ekspertami i rzeczoznawcami
- Bardzo dobra znajomość budynków o różnej specyfice
- Doświadczeni audytorzy

Chcesz zamówić audyt PPOŻ.? Skontaktuj się z nami!

tel. 22 517 88 66

seka.pl

handlowy@seka.pl

Restrukturyzacja zatrudnienia

kryteria doboru jako element konieczny przyczyny wypowiedzenia

Polskie prawo pracy nakierowane jest przede wszystkim na zabezpieczenie interesów pracowników. Dlatego pracodawcy, chcąc zachować równowagę, muszą być dobrze przygotowani do zgodnego z prawem zabezpieczania realizacji swoich celów.

Aktualnie wielu pracodawców staje przed wyzwaniami związanymi z różnymi formami restrukturyzacji zatrudnienia. Robert Maliszewski – Dyrektor Działu Prawa Pracy SEKA S.A. tłumaczy, jak ustalać kryteria doboru pracowników przy kwalifikowaniu ich do zwolnienia podczas restrukturyzacji.

ROBERT MALISZEWSKI
DYREKTOR DZIAŁU PRAWA PRACY SEKA S.A.

Nawet bez wnikliwej analizy sytuacji na rynku pracy można postawić tezę, że aktualnie coraz więcej pracodawców przeprowadza lub rozważa w najbliższym czasie różne formy restrukturyzacji zatrudnienia.

Jednym z trudniejszych aspektów prawnych w tym zakresie jest dokonanie prawidłowego i zgodnego z prawem doboru konkretnych pracowników, których stanowiska zostaną zlikwidowane i w konsekwencji otrzymają oni wypowiedzenia umów o pracę albo też tzw. wypowiedzenia zmieniające (w trybie art. 42 k.p). Proces ten dotyczy zarówno tzw. zwolnień grupowych, jak i pojedynczych likwidacji stanowisk pracy w oparciu o przepisy ustawy

z dnia 13 marca 2003 r. o szczególnych zasadach rozwiązywania z pracownikami stosunków pracy z przyczyn niedotyczących pracowników (t.j. Dz.U. z 2024, poz. 61.). W artykule przedstawiam orzecznictwo Sądu Najwyższego oraz przykłady doświadczenia, które dostarczają wskazówek, jak ustalać kryteria doboru pracowników przy kwalifikowaniu ich do zwolnienia.

Likwidacja tylko niektórych stanowisk pracy

Wiadomym jest, że wypowiedzając umowę o pracę zawartą

na czas nieokreślony albo określony, należy podać przyczynę takiego wypowiedzenia. Musi być ona prawdziwa, konkretna i dająca się bronić przed sądem.

W przypadku gdy nastąpi likwidacja tylko niektórych stanowisk z kilku takich samych lub podobnych, wówczas oprócz przyczyny wypowiedzenia powinno się w wypowiedzeniu umowy o pracę podać także kryteria doboru, czyli wskazać przesłanki, dlaczego akurat temu konkretnemu pracownikowi wypowiedziana jest umowa o pracę, a nie innemu pracownikowi zatrudnionemu na takim samym lub podobnym stanowisku. Taki obowiązek potwierdza

orzecznictwo Sądu Najwyższego, z analizy którego można wyinterpretować wiele wskazówek, jak taki proces kwalifikacji do zwolnień przeprowadzić. Przykładowo, w wyroku z dnia 4 października 2018 roku (III PK 97/17) Sąd Najwyższy orzekł, że: „potrzeba porównania z innymi pracownikami powstaje wówczas, gdy następuje likwidacja jednego lub kilku spośród większej liczby analogicznych stanowisk i konieczne jest dokonanie wyboru pracowników, z którymi zostanie zakończony stosunek pracy. Wówczas pracodawca ma obowiązek wskazania w wypowiedzeniu umowy o pracę kryteriów doboru pracownika do zwolnienia. Jeżeli bowiem likwidacja



dotyczy tylko jednego albo części spośród większej liczby takich samych lub podobnych stanowisk pracy, to tak określona przyczyna wypowiedzenia (likwidacja stanowiska) tłumaczy konieczność zwolnienia pracownika, ale nie wyjaśnia, dlaczego rozwiązano stosunek pracy z konkretnym pracownikiem, pozostawiając w zatrudnieniu inne osoby zajmujące stanowiska objęte redukcją”.

Bezpieczne kryteria doboru do zwolnienia

W uzasadnieniu wyroku z dnia 12 listopada 2014 roku (I PK 73/14) Sąd Najwyższy wyjaśnił, że w razie indywidualnego

zwolnienia pracownika w związku z likwidacją stanowiska pracy, porównanie jego sytuacji do sytuacji innych pracowników obejmuje takie obiektywne kryteria, jak: staż pracy, wykształcenie, kwalifikacje faktyczne, dotychczasowy przebieg pracy, doświadczenie zawodowe, szczególne umiejętności i predyspozycje do wykonywania pracy określonego rodzaju w ramach tej samej grupy pracowników (zajmujących podobne stanowiska), nie zaś z uwzględnieniem tylko jednej komórki organizacyjnej.

Inne orzeczenie SN, na które należy zwrócić uwagę, to wyrok Sądu Najwyższego – Izba Administracyjna, Pracy i Ubezpieczeń Społecznych z dnia 6 listopada 2001 r. (I PKN 675/00). Czytamy w nim, że w razie podjęcia przez pracodawcę indywidualnej decyzji o rozwiązaniu stosunku pracy z przyczyn organizacyjnych,



Pamiętaj!

Wypowiadając umowę o pracę zawartą na czas nieokreślony albo określony, należy podać przyczynę takiego wypowiedzenia. Musi być ona prawdziwa, konkretna i dająca się bronić przed sądem.

wybór pracownika do zwolnienia powinien być dokonany w oparciu o porównanie sytuacji pracowników w ramach tej samej grupy pracowniczej (osób wykonujących pracę podobną, zajmujących podobne stanowiska), nie zaś z uwzględnieniem sytuacji wszystkich pracowników zatrudnionych w zakładzie pracy albo w jego określonej komórce organizacyjnej.

Zgodnie z postanowieniem SN z 27.11.2018 r. (I PK 250/17, LEX nr 2583104), zasadniczo najważniejszymi kryteriami doboru do zwolnienia powinny być: przydatność pracownika do pracy, jego kwalifikacje i umiejętności zawodowe, doświadczenie zawodowe, staż i przebieg dotychczasowej pracy, dyspozycyjność wobec pracodawcy. Oczywiście pracodawca nie musi nadawać wszystkim kryteriom takiego samego znaczenia, lecz

Proces kwalifikacji do zwolnień

W procesie kwalifikacji pracowników do zwolnień należy poszukać kryteriów doboru, biorąc pod uwagę kryteria obiektywne. Zwykle będą one związane z wykonywaną przez pracownika pracą np.:

- staż pracy lub staż na danym stanowisku,
- wykształcenie,
- specyficzne kwalifikacje wymagane na tym stanowisku,
- wykonywanie przez pracownika obowiązków służbowych,
- nałożenie lub brak kar porządkowych,
- wydajność w pracy,
- jakość i terminowość wykonywania pracy,
- przestrzeganie obowiązujących zasad, przepisów wewnętrznych,
- spóźnianie do pracy,
- obecność w pracy (poziom absencji), itd.

Nie ma jednego, zamkniętego katalogu kryteriów doboru do zwolnienia, w związku z tym trzeba dokładnie przeanalizować potrzeby pracodawcy oraz specyfikę pracy na danym stanowisku.



fot. archiwum SEKA S.A.

staż na danym stanowisku, wykształcenie, specyficzne kwalifikacje wymagane na tym stanowisku, wykonywanie przez pracownika obowiązków służbowych, nałożenie lub brak kar porządkowych, wydajność w pracy, jakość i terminowość wykonywania pracy, przestrzeganie obowiązujących zasad, przepisów wewnętrznych, spóźnianie do pracy, obecność w pracy (poziom absencji) itd. Nie ma jednego, zamkniętego katalogu kryteriów doboru do zwolnienia, w związku z tym trzeba dokładnie przeanalizować potrzeby pracodawcy oraz specyfikę pracy na danym stanowisku. Nic nie stoi na przeszkodzie, aby wybrać kilka istotnych, obiektywnych kryteriów – wedle ustalonej punktacji – przyznać poszczególnym, porównywanym pracownikom punkty za każde kryterium. Po zsumowaniu uzyskanych punktów pracownicy, którzy uzyskali ich najmniej, będą wytypowani do rozwiązania z nimi umów o pracę.

Wskazać należy, iż w przypadku, kiedy likwidacji ma ulec jedno stanowisko pracy, które jest jedynym takim w strukturze danej firmy i nie ma też stanowisk do niego podobnych, wówczas

nie ma obowiązku podawania kryteriów doboru do zwolnienia, przy czym w mojej ocenie należy w treści wypowiedzenia wskazać ten fakt.

Jak widać, opisany proces może być trudny i złożony, a jego nieprawidłowe przeprowadzenie często skutkuje pozwami do sądów pracy i niestety przegrany pracodawców. Warto zatem przed wręczeniem wypowiedzeń skonsultować te i inne kwestie z doświadczonymi prawnikami – specjalistami z zakresu prawa pracy. Zachęcamy do kontaktu z nami i zapoznania się z naszą ofertą na stronie seka.pl. ■

kierując się istotą i celem prowadzonej przez siebie działalności, w związku z którą zatrudnia pracowników, może przypisać niektórym kryteriom prymat nad innymi. Natomiast kryteria odnoszące się do osobistej sytuacji pracownika, jak z jednej strony stan i obowiązek utrzymania rodziny, zwłaszcza samotne wychowywanie dzieci czy niepełnosprawność, z drugiej zaś strony posiadanie innych źródeł dochodów czy łatwość w znalezieniu nowego zatrudnienia, powinny

być brane pod uwagę jedynie pomocniczo.

Jak uniknąć przegranej przed sądem pracy

Podsumowując, w procesie kwalifikacji pracowników do zwolnień należy poszukać kryteriów doboru, biorąc pod uwagę kryteria obiektywne. Zwykle będą one związane z wykonywaną przez pracownika pracą, np. staż pracy lub



Robert Maliszewski

Dyrektor Działu
Prawa Pracy
SEKA S.A.



Doradztwo z prawa pracy



Rozwijaj swój biznes zgodnie
z obowiązującym prawem pracy

Jak możemy Cię wspierać?



Konsultacje
i doradztwo



Audyt
prawa pracy



Negocjacje



Reprezentacja
przed sądem

tel. 22 517 88 44

seka.pl

prawny@seka.pl



Z nami bezpieczniej



- Dostarczamy kompleksowe usługi doradczo-szkoleniowe wspierające bezpieczeństwo prowadzenia biznesu.
- Odciążamy pracodawców w ich obowiązkach, by mogli w pełni skupić się na swoich strategicznych celach biznesowych.
- Zapewniamy eksperckie doradztwo, dopasowane do potrzeb firmy szkolenia oraz outsourcing usług, by pomagać naszym Klientom umacniać ich pozycję na rynku.



Outsourcing
BHP i PPOŻ.



Doradztwo
z prawa pracy



Outsourcing
szkoleń



Obsługa kadrowo-
płacowo-księgową



Szkolenia
i uprawnienia zawodowe



Ochrona
środowiska



Projekty
unijne



Zarządzanie
bezpieczeństwem

seka.pl

magazyn.seka.pl