ZWIĄZEK PRACODAWCÓW POLSKA MIEDŹ
THE POLISH COPPER EMPLOYERS' ASSOCIATION

Monitoring Legislacji Międzynarodowej

Monitoring działań w UE (legislacja, publikacje) – 8 marca 2024 r.

- **Informacje generalne o prawie UE – akty prawne i dokumenty strategiczne**

Cyberbezpieczeństwo sieci i systemów informatycznych – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywa NIS)

Dyrektywa ma zastosowanie od dnia 8 sierpnia 2016 r. Państwa UE włączają ją do prawa krajowego do dnia 9 maja 2018 r., zaś do dnia 9 listopada 2018 r. dokonują identyfikacji operatorów usług kluczowych.

W dyrektywie przewidziano szeroki wachlarz środków służących zwiększeniu poziomu bezpieczeństwa sieci i systemów informatycznych (cyberbezpieczeństwo) z myślą o zabezpieczeniu usług istotnych dla gospodarki UE oraz społeczeństwa. Służy ona zapewnieniu, że państwa UE są należycie przygotowane i gotowe do podejmowania działań w razie wystąpienia cyberataków i reagowania na nie, a ponadto wprowadza obowiązek:

- wyznaczenia właściwych organów,
- ustanowienia zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), oraz
- przyjęcia krajowych strategii cyberbezpieczeństwa.

Cyberbezpieczeństwo to odporność sieci i systemów informatycznych na działania naruszające dostępność, autentyczność, integralność lub poufność danych cyfrowych lub usług świadczonych poprzez te systemy.

Zgodnie z dyrektywą współpraca na szczeblu unijnym ma dotyczyć wymiaru zarówno strategicznego, jak i technicznego. Wreszcie dyrektywa nakłada na operatorów usług kluczowych i dostawców usług cyfrowych obowiązek wprowadzania stosownych środków bezpieczeństwa oraz zgłaszania poważnych incydentów odpowiednim organom krajowym.

Państwa UE:

- wyznaczają co najmniej jeden właściwy organ krajowy oraz CSIRT, a także pojedynczy punkt kontaktowy (jeśli właściwy jest więcej niż jeden organ);
- identyfikują operatorów usług kluczowych w krytycznych sektorach, takich jak energetyka, transport, finanse, bankowość, służba zdrowia, woda i infrastruktura cyfrowa, w których cyberatak mógłby zakłócić usługę kluczową.

Państwa UE są także zobowiązane do wdrożenia krajowej strategii cyberbezpieczeństwa dla sieci i systemów informatycznych, która obejmuje następujące zagadnienia:

- przygotowanie i gotowość do podejmowania działań w razie wystąpienia cyberataków i reagowania na nie;
- role i zakresy obowiązków organów rządowych i innych podmiotów, a także współpracę między nimi;
- programy edukacyjne, informacyjne i szkoleniowe;
- plany badawczo-rozwojowe;
- planowanie z myślą o określeniu ryzyk.

Sieci i systemy informatyczne to sieć łączności elektronicznej lub wszelkie urządzenia lub grupy wzajemnie połączonych urządzeń, które przetwarzają dane cyfrowe, a także przechowywane, przetwarzane, odzyskiwane lub przekazywane dane cyfrowe.

Właściwe organy krajowe monitorują stosowanie dyrektywy:

- oceniając politykę cyberbezpieczeństwa i bezpieczeństwa stosowaną przez operatorów usług kluczowych;
- nadzorując dostawców usług cyfrowych;
- uczestnicząc w pracach grupy współpracy (w której skład wchodzą właściwe organy odpowiedzialne za bezpieczeństwo sieci i informacji z każdego z państw UE, Komisja Europejska oraz Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA));
- przekazując ogółowi społeczeństwa, przy zachowaniu poufności, informacje niezbędne do zapobieżenia incydentowi lub poradzenia sobie z trwającym incydentem;
- wydając wiążące polecenia w celu zaradzenia uchybieniom w dziedzinie cyberbezpieczeństwa.

Zadania CSIRT obejmują:

- monitorowanie cyberincydentów i reagowanie na nie;
- zapewnianie analizy ryzyka i incydentów oraz orientacji sytuacyjnej;
- udział w sieci CSIRT;
- współpracę z sektorem prywatnym;
- wspieranie stosowania znormalizowanych praktyk w odniesieniu do postępowania w przypadku incydentu i wystąpienia ryzyka oraz klasyfikacji informacji.

Celem dyrektywy jest propagowanie kultury zarządzania ryzykiem. Przedsiębiorstwa prowadzące działalność w najważniejszych sektorach muszą dokonać oceny ryzyka, na jakie są narażone, a także podjąć działania pozwalające zapewnić cyberbezpieczeństwo. Zgłaszają one właściwym organom lub CSIRT wszelkie istotne incydenty, takie jak włamania lub przypadki kradzieży danych, które w sposób poważny naruszają cyberbezpieczeństwo i mają istotny skutek zakłócający dla ciągłości usług krytycznych i dostaw towarów.

Przy określaniu, które incydenty mają być zgłaszane przez operatorów usług kluczowych, państwa UE biorą pod uwagę czas trwania i zasięg geograficzny incydentu, a także inne czynniki, na przykład liczbę użytkowników korzystających z danej usługi. Usługi kluczowe to usługi świadczone przez przedsiębiorstwa prywatne lub jednostki publiczne, które spełniają ważną rolę w społeczeństwie i gospodarce (np. zaopatrzenie w wodę, usługi energetyczne itp.).

Najważniejsi dostawcy usług cyfrowych (wyszukiwarek, usług przetwarzania w chmurze i internetowych platform handlowych) również będą musieli spełnić wymogi dotyczące bezpieczeństwa i zgłaszania incydentów.

Na mocy dyrektywy ustanawia się grupę współpracy, której zadania obejmują:

- udzielanie wskazówek dotyczących działalności sieci CSIRT;
- wymianę najlepszych praktyk dotyczących identyfikowania operatorów usług kluczowych;
- pomaganie państwom UE w budowaniu zdolności w zakresie cyberbezpieczeństwa;
- wymianę informacji i najlepszych praktyk dotyczących podnoszenia świadomości i szkolenia oraz badań i rozwoju;
- wymianę informacji i gromadzenie informacji z zakresu najlepszych praktyk dotyczących ryzyk i incydentów;

- omawianie zasad dotyczących zgłaszania incydentów.

W dyrektywie ustanawia się także sieć CSIRT, która składa się z przedstawicieli CSIRT z państw UE oraz zespołu reagowania na incydenty komputerowe (CERT–EU). Jej zadania obejmują:

- wymianę informacji dotyczących usług CSIRT;
- wymianę informacji dotyczących cyberincydentów;
- zapewnianie państwom UE wsparcia w zakresie reagowania na incydenty transgraniczne;
- omawianie i określanie skoordynowanej reakcji na incydent zgłoszony przez państwo UE;
- omawianie, badanie i określanie dalszych form współpracy operacyjnej, w tym w odniesieniu do:
    - kategorii ryzyk i incydentów;
    - wczesnego ostrzegania;
    - wzajemnej pomocy;
    - koordynacji w przypadku gdy państwa reagują na ryzyka i incydenty dotyczące więcej niż jednego państwa UE;
- informowanie grupy współpracy o swoich działaniach i zwracanie się o wskazówki;
- omawianie wniosków z ćwiczeń w zakresie cyberbezpieczeństwa;
- omawianie zdolności danego CSIRT (na jego wniosek);
- wydawanie wytycznych dotyczących współpracy operacyjnej.

Państwa UE stosują skuteczne, proporcjonalne i odstraszające sankcje w celu zapewnienia stosowania przepisów dyrektywy.

Więcej informacji:
https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016L1148

- **Prowadzone procesy konsultacyjne, projekty, stanowiska:**

1. Dyrektywa w sprawie europejskiej rady zakładowej (zmiana)

Konsultacje publiczne przepisów prawa pracy UE (europejska rada zakładowej) – ocena na podstawie analizy Dyrektywy 2009/38/WE Parlamentu Europejskiego i Rady z dnia 6 maja 2009 r. w sprawie ustanowienia europejskiej rady zakładowej lub trybu informowania pracowników i konsultowania się z nimi w przedsiębiorstwach lub w grupach przedsiębiorstw o zasięgu wspólnotowym oraz Dyrektywy 2002/14/WE Parlamentu Europejskiego I Rady z dnia 11 marca 2002 r. ustanawiająca ogólne ramowe warunki informowania i przeprowadzania konsultacji z pracownikami we Wspólnocie Europejskiej w kontekście Europejskiego filaru praw socjalnych – wniosek w sprawie dyrektywy zmieniającej dyrektywę 2009/38/WE w zakresie ustanawiania i działania europejskich rad zakładowych oraz skutecznego egzekwowania prawa do ponadnarodowego informowania i konsultacji – Etap legislacyjny – Przyjęcie przez Komisję. Ostateczny termin na przesłanie opinii to 15 kwietnia 2024 r.

W trwającej transformacji świata pracy, która jest spowodowana dążeniem do zrównoważenia środowiskowego, gospodarczego i społecznego oraz wdrażaniem nowych technologii, znaczące zaangażowanie pracowników i ich przedstawicieli na wszystkich szczeblach może pomóc w przewidywaniu zmian i zarządzaniu nimi, zmniejszeniu utraty miejsc pracy, utrzymaniu zdolności do zatrudnienia oraz ograniczeniu wpływu na systemy opieki społecznej

i związanych z nim kosztów dostosowania. W przedsiębiorstwach lub grupach wielonarodowych informowanie pracowników i konsultowanie się z nimi na szczeblu ponadnarodowym może w istotny sposób przyczynić się do takiego zaangażowania. W tym celu w dyrektywie 2009/38/WE Parlamentu Europejskiego i Rady („dyrektywa" lub „dyrektywa 2009/38/WE") ustanowiono minimalne wymogi dotyczące tworzenia i funkcjonowania organów reprezentujących pracowników w niektórych przedsiębiorstwach wielonarodowych, tzw. europejskich rad zakładowych. Europejskie rady zakładowe oraz tryby ponadnarodowego informowania pracowników i konsultowania się z nimi uzupełniają informowanie pracowników i konsultowanie się z nimi na szczeblu krajowym.

Wniosek ma na celu wyeliminowanie niedociągnięć dyrektywy, a tym samym poprawę skuteczności ram informowania pracowników i konsultowania się z nimi na szczeblu ponadnarodowym. Nie ma to wpływu na unijne i krajowe przepisy i praktyki dotyczące zaangażowania pracowników na szczeblu krajowym.

Europejskie rady zakładowe są organami informacyjnymi i konsultacyjnymi reprezentującymi unijnych pracowników w przedsiębiorstwach międzynarodowych, które prowadzą działalność w co najmniej dwóch krajach UE.

Celem inicjatywy jest:

- wzmocnienie europejskich rad zakładowych;
- zapewnienie im możliwość skuteczniejszego korzystania z prawa do informowania i prowadzenia konsultacji;
- skuteczniejsze egzekwowania ich praw.

Prawo pracowników do informacji i konsultacji w ramach przedsiębiorstwa określono w Karcie praw podstawowych Unii Europejskiej (art. 27). Traktat o funkcjonowaniu Unii Europejskiej (TFUE) stanowi, że UE wspiera i uzupełnia działania państw członkowskich w dziedzinie informowania pracowników i konsultowania się z nimi (art. 153), promuje dialog społeczny między partnerami społecznymi (art. 151) oraz uznaje rolę partnerów społecznych (art. 152). Zasada 8 Europejskiego filaru praw socjalnych stanowi, że „pracownicy lub ich przedstawiciele mają prawo do uzyskiwania informacji i wyrażania swojej opinii w odpowiednim czasie w dotyczących ich kwestiach".

Link: https://pracodawcy.pl/dyrektywa-w-sprawie-europejskiej-rady-zakladowej-zmiana/

2. Innowacyjne formy wykorzystania energii słonecznej – zalecenie dotyczące promowania ich rozwoju

Konsultacje publiczne przepisów prawa dot. energii w UE (OZE) – ocena na podstawie analizy Dyrektywy 2018/2001 z dnia 11 grudnia 2018 r. w sprawie promowania stosowania energii ze źródeł odnawialnych oraz Dyrektywy Parlamentu Europejskiego i Rady (UE) 2023/2413 z dnia 18 października 2023 r. zmieniająca dyrektywę (UE) 2018/2001, rozporządzenie (UE) 2018/1999 i dyrektywę 98/70/WE w odniesieniu do promowania energii ze źródeł odnawialnych oraz uchylająca dyrektywę Rady (UE) 2015/652 w kontekście Komunikatu KE: Strategii UE na rzecz energii słonecznej – I Etap legislacyjny – Zaproszenie do zgłaszania uwag. Ostateczny termin na przesłanie opinii to 2 kwietnia 2024 r.

Strategia UE na rzecz energii słonecznej, przyjęta w 2022 r. w ramach planu REPowerEU, ma na celu przyspieszenie rozwoju energii słonecznej, w tym innowacyjnych form wytwarzania, aby przyczynić się do stopniowego uniezależnienia UE od rosyjskich paliw kopalnych i osiągnąć ambitne cele REPowerEU w zakresie energii ze źródeł odnawialnych.

W 2023 r. zmieniono dyrektywę (UE) 2018/2001 w sprawie promowania stosowania energii ze źródeł odnawialnych. W dyrektywie zmieniającej (UE) 2023/2413, która weszła w życie 20 listopada 2023 r., zwiększono wiążący unijny cel w zakresie energii ze źródeł odnawialnych

do 42,5 % do 2030 r., przy czym dąży się do osiągnięcia 45%. Energia słoneczna będzie odgrywać kluczową rolę w osiągnięciu tego celu, zgodnie ze zaktualizowanymi projektami krajowych planów w dziedzinie energii i klimatu państw członkowskich.

W strategii UE na rzecz energii słonecznej określono ambitne cele w zakresie wytwarzania energii słonecznej na lata 2025 i 2030 oraz przewidziano, że aby je osiągnąć, UE musi zainstalować średnio około 45 GWAC mocy wytwórczych rocznie w ciągu tego dziesięciolecia.

W strategii UE na rzecz energii słonecznej stwierdza się, że innowacyjne formy wykorzystania energii słonecznej będą musiały odgrywać ważną i coraz większą rolę, aby osiągnąć cele UE w zakresie energii odnawialnej. W strategii określono pięć rodzajów form wykorzystania energii słonecznej: agrofotowoltaika, fotowoltaika pływająca, fotowoltaika przy infrastrukturze transportowej, fotowoltaika zintegrowana z budynkiem i fotowoltaika zintegrowana z pojazdem.

Aby wyeliminować przeszkody utrudniające upowszechnianie się tych form wykorzystania energii słonecznej, Komisja wyda, oprócz zalecenia, wytyczne dla państw członkowskich.

Link: https://pracodawcy.pl/innowacyjne-formy-wykorzystania-energii-slonecznej-zalecenie-dotyczace-promowania-ich-rozwoju/

- **Publikacje oraz inne informacje:**

1. Webinar: Możliwości Inwestycyjne w Ukrainie dla polskich firm

Związek Przedsiębiorców i Pracodawców zaprasza na webinar: “Możliwości Inwestycyjne w Ukrainie dla polskich firm”, na mocy Ustawy Ukrainy „O państwowym wsparciu projektów inwestycyjnych ze znaczącymi inwestycjami w Ukrainie“, który odbędzie się 13 marca 2024 r. w godz. 14:00-15:00 (czas polski), 15:00-16:00 (czas ukraiński) na platformie ZOOM.

Webinar jest skierowany do polskich przedsiębiorców zainteresowanych rozwojem swojej działalności na terenie Ukrainy. Wydarzenie skupi się na prezentacji możliwości inwestycyjnych w Ukrainie. Podczas sesji, Nazar Kohut, doświadczony doradca inwestycyjny w UkraineInvest, przedstawi kluczowe aspekty i korzyści płynące z państwowego wsparcia dla zagranicznych inwestorów.

Prelegent: Nazar Kohut – Doradca Inwestycyjny w UkraineInvest, rządowym biurze ds. pozyskiwania i wspierania inwestycji w Ukrainie.

Tematy webinaru:

- Wsparcie Państwowe: Omówienie form wsparcia oferowanych przez ukraiński rząd dla inwestorów zagranicznych.
- Wymagania dotyczące projektów: Kryteria, które muszą spełniać projekty inwestycyjne, aby kwalifikować się do wsparcia.
- Zdolność finansowa: Jakie zasoby finansowe są potrzebne, aby rozpocząć projekt inwestycyjny na Ukrainie.
- Wymagane dokumenty: Przegląd dokumentacji niezbędnej do aplikacji o wsparcie państwowe.
- Procedura składania wniosku: Krok po kroku przez proces aplikacyjny, aby zwiększyć szanse na sukces.

Udział w webinarze jest bezpłatny.

Organizatorzy: ZPP, Business for Ukraine Center, SUP, InfoCredit.

Partnerzy merytoryczni: Ukraineinves, InfoCredit, Diia.Business.

Wydarzenie realizowane we współpracy Związku Pracodawców i Przedsiębiorców z Fundacją Totalizatora Sportowego.

Link: https://pracodawcy.pl/webinar-mozliwosci-inwestycyjne-w-ukrainie-dla-polskich-firm/

2. VI Kongres MIT Sloan Management Review Polska

ICAN Institute oraz MITSloan Management Review Polska zapraszają na VI Kongres MIT Sloan Management Review Polska, który odbędzie się w formule online w dniach 21-22 marca 2024 roku.

Jak AI dyktuje przyszłość biznesu? Co na to eksperci?

To już 6. edycja najważniejszego wydarzenia technologiczno-biznesowego w Europie Środkowo-Wschodniej.

Tematy:

- Etyka w AI i sztuczna inteligencja w Metaverse
- Rozwój ekologicznych technologii
- Generatywna sztuczna inteligencja i przyszłość zarządzania
- AI w badaniach rynku: szanse i ograniczenia
- Reskilling, rozwój pracowników i kompetencje przyszłości
- ESG jako narzędzie przewagi konkurencyjnej
- Różnorodność pokoleń i neuroatypowi w miejscu pracy

W trakcie wydarzenia:

- 2 Inspirujące ścieżki tematyczne: Innowacyjność w dobie AI oraz Przyszłość pracy
- Sesje Q&A ze światowymi ekspertami (zapewniamy tłumaczenie symultaniczne)
- Dostęp do materiałów z wydarzenia ważny aż 6 miesięcy
- Dodatkowy zastrzyk wiedzy, czyli e-book „Otwarta strategia”
- Rozpoznawalny certyfikat potwierdzający zdobycie wiedzy

W wydarzeniu można wziąć bezpłatny udział lub skorzystać z płatnego pakietu z dodatkowymi korzyściami.

2 dni pełne inspirujących wystąpień ekspertów z całego świata. Trendy zmieniające biznes i odpowiedzi na ważne pytania. Czy AI jest etyczne? Czy Metaverse ma potencjał ekonomiczny w Polsce? Jak technologie zmienią sposób zarządzania ludźmi i firmami?

Link: https://pracodawcy.pl/vi-kongres-mit-sloan-management-review-polska/

3. Jak efektywnie rozwijać cyberbezpieczeństwo w scyfryzowanym świecie? 20.03.2024 g. 9:30 – webinar – Akademia Rozwoju Przemysłu 4.0

Związek Pracodawców Polska Miedź, EXATEL S.A. oraz Polski Klaster IoT & AI SINOTAIC

zapraszają na webinar: „Jak efektywnie rozwijać cyberbezpieczeństwo w scyfryzowanym świecie?” w ramach projektu Akademia Rozwoju Przemysłu 4.0.

Udział w webinarze jest BEZPŁATNY. Wystarczy się zarejestrować, aby otrzymać dostęp do udziału w wydarzeniu

Cyberbezpieczeństwo to metody zmniejszenia przez organizację ryzyka cyberataków, ich realnego wpływu na działalność oraz sposoby ochrony używanych urządzeń i usług.

Cyberbezpieczeństwo to także strategie służące ochronie zasobów cyfrowych przed zhakowaniem.

Cyberbezpieczeństwo staje się kluczowe, ponieważ smartfony, komputery i tablety stały się nieodłącznym elementem naszej codziennej pracy i życia osobistego. Opieranie się na narzędziach online w różnych aspektach prowadzenia biznesu – od mediów społecznościowych i marketingu e-mailowego po przechowywanie danych o pracownikach i klientach w chmurze – oznacza dla nas konieczność ochrony tych informacji.

Postępująca cyfryzacja naszego świata stwarza nowe możliwości dla firm/instytucji w różnych aspektach funkcjonowania. Jednak wraz z nimi pojawiają się też zagrożenia dla bezpieczeństwa w sieci. Według statystyk średni koszt uporania się z cyberatakiem może wynieść około 200 000 dolarów, bez względu na wielkość firmy. To sprawia, że ok. 60% ofiar zamyka działalność w ciągu pół roku po takim ataku z powodu trudności finansowych. Wiedza o cyberbezpieczeństwie i są niezwykle ważne w uchronieniu nowej lub dłużej działającej firmy przed ryzykiem zhakowania. Znaczne zagrożenie istnieje w małych i średnich przedsiębiorstwach. Według raportu Federacji Małego Biznesu („The Federation of Small Businesses") z Wielkiej Brytanii ten rodzaj firm jest atakowany ponad 7 milionów razy rocznie, co kosztuje angielską gospodarkę 5.3 bilionów £.

Solidna wiedza o cyberbezpieczeństwie jest kluczowa, ponieważ ataki stale się rozwijają i stają się coraz bardziej zaawansowane.

Ataki hakerskie powodują:

- utratę wrażliwych danych;
- duże koszty odzyskania skradzionych danych
- straty finansowe w wyniku kradzieży;
- utratę dobrej reputacji;
- zamknięcie działalności.

Dowiedz się co zrobić, aby nie zostać ofiarą cyberprzestępcy, podczas kolejnego spotkania z cyklu Akademia Rozwoju Przemysłu 4.0

Jak efektywnie rozwijać cyberbezpieczeństwo w scyfryzowanym świecie?, które odbędzie się 20 marca 2024 roku w godzinach 9:30 – 11:00 na platformie zoom.

Cyberbezpieczeństwo jest bardzo ważne i jego znaczenie będzie wzrastać wraz z rozwojem technologii, ponieważ cały świat zmienił się w kierunku cyfrowych usług. Stał się bardziej zdigitalizowany. Usługi finansowe, ochrona zdrowia, transport, energia i każdy znaczący obszar naszego życia będzie w coraz większym stopniu wykorzystywać interakcje oparte na sferze digital (w szczególności w Internet of Things oraz IT).

Jak chronić się przed tak dużą ilością niebezpieczeństw? Jak być smart & secure? Cyberbezpieczeństwo – na jakie obszary zwrócić uwagę w zależności od specyfiki organizacji? Pierwsze kroki, czyli co warto rozważyć w pierwszej kolejności.

Odpowiedzi na te i inne pytania podczas spotkania.

GŁÓWNE TEMATY WEBINARU

1. Cyfryzacja w dzisiejszych czasach – więcej możliwości i … podatności. Jak być smart & secure?
2. Cyberbezpieczeństwo – na jakie obszary zwrócić uwagę w zależności od specyfiki organizacji?
3. Pierwsze kroki, czyli co warto rozważyć w pierwszej kolejności.

Link: https://pracodawcy.pl/cyberbezpieczenstwo/

4. Zalecenia KE w sprawie technologii informacyjno-komunikacyjnych w celu ułatwienia przejścia UE na energooszczędną i niskoemisyjną gospodarkę

Zalecenie Komisji 2013/105/WE z dnia 9 października 2009 r. w sprawie wykorzystania technologii informacyjno-komunikacyjnych (TIK) do ułatwienia przejścia na energooszczędną i niskoemisyjną gospodarkę (L 51/18).

2013/105/EC: Commission Recommendation of 9 October 2009 on mobilising Information and Communications Technologies to facilitate the transition to an energy-efficient, low-carbon economy

Komisja Europejska sporządziła szereg zaleceń dla sektora technologii informacyjno-komunikacyjnych (TIK) i dla państw członkowskich, by pomóc UE w przejściu na energooszczędną i niskoemisyjną gospodarkę. Komisja Europejska opracowała dwa zestawy zaleceń, jeden dla sektora TIK, drugi dla państw członkowskich, by ułatwić przejście UE na energooszczędną i niskoemisyjną gospodarkę.

Zalecenia dla sektora TIK

Ogólnym celem sektora TIK jest wykazanie wymiernego i możliwego do sprawdzenia ograniczenia energochłonności i emisji dwutlenku węgla we wszystkich procesach związanych z produkcją, transportem i sprzedażą sprzętu i składników TIK.

Jednym z przykładowych zaleceń dla sektora TIK jest określenie rozwiązań TIK pozwalających na zwiększenie efektywności energetycznej nowych i istniejących budynków oraz ulepszenie praktyk budowlanych i remontowych.

Kolejnym przykładem jest określenie, w bliskiej współpracy z sektorem transportu i logistyki, rozwiązań TIK pozwalających na zwiększenie efektywności energetycznej i ekologiczności usług tego sektora.

Ponadto Komisja zaleciła, by sektor TIK przyjął wspólne metody pomiaru efektywności energetycznej i emisji dwutlenku węgla do 2020 r.

Zalecenia dla państw członkowskich

Komisja zaleca m. in., by państwa członkowskie stosowały rozwiązania oparte na TIK do celów poprawy efektywności energetycznej.

Inteligentne systemy pomiarowe

Inteligentne sieci i inteligentne systemy pomiarowe mogą zwiększyć efektywność i kontrolę produkcji, a także poprawić dystrybucję i zużycie energii. Państwa członkowskie do końca 2010 r. miały ustalić wspólną minimalną specyfikację funkcjonalną inteligentnych systemów pomiarowych, dostarczającą konsumentom lepszych informacji na temat zużycia energii i lepszych metod zarządzania tym zużyciem. Na przykład dzięki zainstalowaniu inteligentnych systemów pomiarowych w domach konsumenci mogli obniżyć zużycie energii aż o 10%. W 2012 r. Komisja sporządziła wykaz projektów dotyczących inteligentnych sieci i inteligentnych systemów pomiarowych w Europie. Obejmuje on 281 projektów dotyczących inteligentnych sieci oraz około 90 projektów dotyczących pilotażowych inteligentnych systemów pomiarowych i wdrożeń z 30 krajów w Europie.

Stosowanie TIK do symulacji i modelowania w zakresie energii

Organy administracji publicznej państw członkowskich na poziomie krajowym, regionalnym i lokalnym są zachęcane do lepszego wykorzystania narzędzi TIK do symulacji i modelowania w zakresie energii, w tym podczas szkolenia specjalistów w sektorach budownictwa, transportu i logistyki.

Kolejną propozycją dla państw członkowskich jest zwiększenie stosowania bardziej efektywnych energetycznie technologii przez włączenie ich do programów zamówień publicznych.

Link: https://pracodawcy.pl/zalecenia-ke-w-sprawie-technologii-informacyjno-komunikacyjnych-w-celu-ulatwienia-przejscia-ue-na-energooszczedna-i-niskoemisyjna-gospodarke/

Źródło: EUR-Lex, Komisja Europejska, Związek Przedsiębiorców i Pracodawców, Business for Ukraine Center, ICAN sp. z o.o. sp.k., MITSloan Management Review Polska, EXATEL S.A., Polski Klaster IoT & AI SINOTAIC