OCHRONA DANYCH OSOBOWYCH

Ocena ryzyka i skutków
Metody i praktyczne przykłady

redakcja Mirosław Gumularz, Tomasz Izydorczyk

Marcin Błoński, Mirosław Gumularz, Tomasz Izydorczyk
Maciej Kołodziej, Beata Konieczna-Drzewiecka
Maciej Otmianowski, Monika Sobczyk, Mariola Więckowska

PRAWO W PRAKTYCE

Wolters Kluwer

OCHRONA DANYCH OSOBOWYCH

Ocena ryzyka i skutków
Metody i praktyczne przykłady

redakcja Mirosław Gumularz, Tomasz Izydorczyk

Marcin Błoński, Mirosław Gumularz, Tomasz Izydorczyk
Maciej Kołodziej, Beata Konieczna-Drzewiecka
Maciej Otmianowski, Monika Sobczyk, Mariola Więckowska

PRAWO W PRAKTYCE

Zamów książkę w księgarni internetowej
profinfo.pl
księgarnia internetowa

Wolters Kluwer

WARSZAWA 2021

Stan prawny na 1 lutego 2021 r.

Recenzent
Dr hab. Agnieszka Grzelak, prof. ALK

Wydawca
Monika Pawłowska

Redaktor prowadzący
Małgorzata Jarecka

Opracowanie redakcyjne
JustLuk

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

Poszczególne części napisali:
Marcin Błoński i Maciej Otmianowski – praktyczny przykład nr 14
Mirosław Gumularz – rozdział 5, praktyczny przykład nr 1
Mirosław Gumularz, Tomasz Izydorczyk – rozdziały 1– 4, rozdział 7
Tomasz Izydorczyk – rozdział 6, praktyczne przykłady nr. 2–8
Beata Konieczna-Drzewiecka – praktyczne przykłady nr. 12 i 13
Maciej Kołodziej – praktyczny przykład nr 9
Monika Sobczyk – praktyczny przykład nr 10
Mariola Więckowska – praktyczny przykład nr 11

prawolubni

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegał przysługujących im praw. Książkę możesz udostępnić osobom bliskim lub osobiście znanym, ale nie publikuj jej w internecie. Jeśli cytujesz fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A jeśli musisz skopiować część, rób to jedynie na użytek osobisty.

Szanujmy prawo i własność
Więcej na www.legalnakultura.pl
Polska Izba Książki

© Copyright by Wolters Kluwer Polska Sp. z o.o., 2021

ISBN 978-83-8223-533-3

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

1. Akty prawne

k.c.	– ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2020 r. poz. 1740 ze zm.)
k.p.	– ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2020 r. poz. 1320 ze zm.)
k.p.a.	– ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2020 r. poz. 256 ze zm.)
pr. tel.	– ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2019 r. poz. 2460 ze zm.)
RODO	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1, ze zm.)
u.o.d.o.	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 ze zm.)
u.p.p.	– ustawa z 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2020 r. poz. 849)
ustawa covidowa	– ustawa z 2.03.2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. z 2020 r. poz. 1842 ze zm.)
u.ś.u.d.e.	– ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344 ze zm.)

2. Inne

AEPD	– Agencia Española de Protección de Datos
CNIL	– Commission nationale de l'informatique et des libertés
EIOD	– Europejski Inspektor Ochrony Danych Osobowych
ENISA	– Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji

EROD	– Europejska Rada Ochrony Danych
GIODO	– Generalny Inspektor Ochrony Danych Osobowych
GR29	– Grupa Robocza art. 29
ICO	– Information Commissioner's Office
IZSI	– instrukcja zarządzania systemami informatycznymi
LIA	– legitimate interests assessment
M. Praw.	– Monitor Prawniczy
NSA	– Naczelny Sąd Administracyjny
OSOD	– ocena skutków dla ochrony danych
RCP	– rejestr czynności przetwarzania
SLA	– Service Level Agreement
UODO	– Urząd Ochrony Danych Osobowych
WHO	– Światowa Organizacja Zdrowia
WSA	– wojewódzki sąd administracyjny

Praktyczny przykład nr 11

ZARZĄDZANIE FLOTĄ

Autor: Mariola Więckowska

Studium przypadku: zarządzanie flotą samochodową (System Ekojazda)

W przypadku **wysokiego ryzyka** naruszenia praw lub wolności osoby fizycznej, zgodnie z art. 35 RODO, należy przeprowadzić ocenę skutków dla ochrony danych – OSOD (ang. *Data Privacy Impact Assessment* – DPIA).

Ocena skutków dla ochrony danych to proces, który należy dostosować do zasad ochrony danych obowiązujących w organizacji i który pozwoli na ich bezpieczne przetwarzanie, m.in. przez podjęcie kluczowych decyzji już w fazie projektowania (*privacy by design*), domyślną ochronę danych (*privacy by default*) oraz wczesne zaadresowanie i minimalizację potencjalnych ryzyk prywatności (*risk bassed approach*).

OSOD pozwoli na:
- wykazanie zgodności z RODO;
- opracowanie strategii ograniczenia ryzyka dla ochrony danych osobowych;
- wsparcie organizacji w identyfikowaniu oraz minimalizowaniu ryzyka związanego z ochroną prywatności podczas pracy nad nowymi projektami lub regulacjami;
- identyfikację potencjalnych problemów na bardzo wczesnym etapie i ułatwienie ich rozwiązywania, a tym samym – obniżenie kosztów;
- uniknięcie drogich i czasochłonnych zmian, opóźnień i ryzyka niepowodzenia projektu;
- postępowanie zgodnie z ogólnie przyjętymi zasadami etyki;
- ochronę przed utratą reputacji.

Terminologia OSOD często odwołuje się do wprowadzania znaczących zmian w istniejącej czynności przetwarzania danych lub rozpoczyna nową czynność ich przetwarzania. W związku z tym powinna być szeroko interpretowana do wdrożenia nowego systemu informatycznego, po wykorzystanie już przetwarzanych danych do nowego celu przetwarzania.

Praktyka pokazuje, że proces oceny skutków dla ochrony danych warto udokumentować w procedurze, którą należy wdrożyć w organizacji. Przyjęte zasady należy w szczególności przekazać osobom odpowiedzialnym za wprowadzanie zmian. Warto również opracować przykładową listę zmian, które powinny być konsultowane z IOD w fazie jej projektowania.

Ryzyko prywatności związane z naruszeniem praw lub wolności osób może wynikać m.in. z przetwarzania danych osobowych, które są:
- błędne, niewystarczające lub nieaktualne;
- nadmiarowe lub nieistotne;
- przechowywane zbyt długo;
- ujawniane nieupoważnionym osobom;
- wykorzystywane nieetycznie, w sposób ogólnie nieakceptowalny lub w sposób, którego osoby, których dane dotyczą, się nie spodziewały;
- przetwarzane w sposób niedostatecznie bezpieczny.

Etap 1. Ogólna analiza ryzyka – wymagana dla każdej zmiany

Ustalenie, czy we wprowadzanej zmianie będzie dochodziło do przetwarzania danych osobowych oraz czy będzie ona stwarzała z dużym prawdopodobieństwem **wysokie ryzyko** naruszenia praw lub wolności osób – wtedy **dalsze etapy OSOD będą wymagane**.

W tym etapie ustala się m.in.:
- dlaczego wprowadzamy zmianę (np. polepszenie usługi, zwiększenie wydajności, poprawa ochrony prywatności);
- jaka jest podstawa prawna zmiany;
- zakres przetwarzanych danych wraz z ich celem i charakterem;
- kategorie przetwarzanych danych: ogólnie dostępne, zwykłe, szczególne;
- skutki łączenia informacji z innymi danymi;
- nośniki danych, np. papier, dane elektroniczne i ich rodzaj;
- użycie nowych technologii;
- ocenę poziomu ryzyka i związaną z tym decyzję o przeprowadzeniu pełnego OSOD.

Przykładowa dokumentacja tego etapu:

Zarządzanie flotą samochodową: wstępna ocena skutków dla ochrony danych – ogólna analiza ryzyka

Informacje o procesie przetwarzania oraz dane administratora	
Administrator	**Firma X sp. z o.o.**
Właściciel biznesowy procesu	Jan Nowak, jan.nowak@firmax.pl
Opiekun procesu	Jan Kowalski, jan.kowalski@firmax.pl
Czynność przetwarzania/proces (nazwa procesu zgodnie z rejestrem czynności przetwarzania)	zarządzanie flotą samochodową (Ekojazda)

ETAP 0. STAN FAKTYCZNY	
1. Opis stanu faktycznego	Wdrożenie systemu do zarządzania flotą samochodów w następujących celach głównych: • zapewnienia większego bezpieczeństwa na drodze pracownikom Firmy X; • możliwość lepszego rozliczenia kilometrówek w relacji pracownik – pracodawca oraz dodatkowo działania proekologiczne. System Ekojazda w oparciu o sztuczną inteligencję i przy wykorzystaniu technologii *Big Data* i uczenia maszynowego pozwoli Firmie X zautomatyzować procesy zarządzania i administrowania flotą samochodową oraz zwiększy bezpieczeństwo pracowników podczas jazdy samochodem służbowym. W procesie dochodzi do zaawansowanej analizy techniki jazdy przez detekcję i analizę ponad 800 różnych zdarzeń związanych z użytkowaniem samochodu, które przekładają się na bezpieczeństwo na drodze. System Ekojazda w prosty i zautomatyzowany sposób komunikuje się z pracownikami, którzy na bieżąco mają dostęp do pełnych informacji dotyczących ich jazdy i tras. Od godziny 8.00 do 16.00 z automatu wszystkie trasy są zaznaczane jako służbowe, jednak pracownik sam może oznaczyć przejazd jako prywatny. Poza wskazanymi godzinami pracownik może dodatkowo oznaczyć jako służbowy przejazd, który pierwotnie był traktowany jako prywatny. **Pracodawca ma dostęp tylko do tras oznaczonych przez pracownika jako służbowe. Trasy prywatne są widoczne jedynie dla pracownika – pracodawca w raporcie potrzebnym do rozliczeń z pracownikiem dostaje informację tylko o liczbie przejechanych prywatnie kilometrów.** Ponieważ jednym z celów jest zapewnienie bezpiecznej jazdy, każdy z pracowników widzi, czy jeździ bezpiecznie – ocenie podlega wiele czynników i zachowań kierowcy, w tym m.in. odpowiednie hamowanie, prędkość oraz spalanie paliwa porównywane z danymi statystycznymi samochodu pobranymi z baz otwartych producentów samochodu. Pracownik na bieżąco informowany jest o postępach w swoich jazdach oraz obszarach, które ze względów bezpieczeństwa wymagają poprawy. Informacje o sposobie jazdy są przetwarzane w sposób całkowicie automatyczny. System Ekojazda ma również wbudowany moduł Konkurs – dostęp do wszystkich osiągniętych i aktywnych wyzwań dla kierowcy w jednym miejscu. Umożliwia on pracownikom jeżdżącym samochodami służbowymi rywalizację

<table>
<tr><td></td><td>w bezpiecznej jeździe, w oparciu o sztuczną inteligencję i uczenie maszynowe. W module tym wbudowane są również konkursy na bezpieczną jazdę oraz możliwość podejrzenia archiwalnych wyników.
System Ekojazda ma również moduł Wiadomości, będący centrum całej komunikacji z kierowcą.
Są też sekcje związane m.in.: ze statystykami, trasami, profilem kierowcy i ustawieniami samochodu.</td></tr>
<tr><td>2. Nazwa przedmiotu oceny</td><td>Przedmiotem oceny jest proces, których przy wykorzystaniu systemu Ekojazda i urządzeń montowanych w samochodach służbowych weryfikuje m.in. jazdę pracowników i pozwala na zwiększenie bezpieczeństwa kierowcy podczas jazdy samochodem.</td></tr>
<tr><td colspan="2">ETAP I. TŁO OCENY RYZYKA</td></tr>
<tr><td>1. Cele przetwarzania</td><td>• zapewnienie pracownikom Firmy X większego bezpieczeństwa na drodze;
• łatwiejszy sposób rozliczania się kierowcy z kilometrówek;
• działania proekologiczne przez promocję bezpiecznego i ekologicznego stylu jazdy;
• zarządzanie flotą samochodów</td></tr>
<tr><td>2. Kontekst przetwarzania</td><td>dane przetwarzane w kontekście administracyjno-pracowniczym, związanym m.in. z czynnościami operacyjnymi i rozliczeniami finansowymi dotyczącymi zarządzaniem flotą samochodową</td></tr>
<tr><td>3. Zakres przetwarzania</td><td>
<table>
<tr><th>Typy danych według ustalonego w organizacji standardu</th><th>Tak / Nie</th><th>Waga</th><th>Proponowana wartość ryzyka</th></tr>
<tr><td>dane osobowe podstawowe</td><td>Tak</td><td>1</td><td>Ryzyko</td></tr>
<tr><td>dane o ograniczonym dostępie/profilowe (np. PESEL, numer karty bankowej, skan dowodu)</td><td></td><td>2</td><td>Ryzyko</td></tr>
<tr><td>dane finansowe/geolokalizacja</td><td>Tak</td><td>3</td><td>Wysokie ryzyko</td></tr>
<tr><td>dane szczególne</td><td></td><td>4</td><td>Wysokie ryzyko</td></tr>
</table>

Zakres przetwarzanych danych osobowych – imię i nazwisko, numer służbowego telefonu, służbowy adres e-mail, lokalizacja samochodu, lokalizacja samochodu w określonym czasie, numer rejestracyjny, dane o eksploatacji pojazdów, w tym zużyciu paliwa, dane o technice i stylu jazdy kierującego, wizualizacja przejechanych tras, czas przejazdu, prędkość, informacje o zdarzeniach, miejsce w konkursie (jeżeli trwa), raporty zbiorcze i zestawienia, login w postaci e-mail, dane z geolokalizacji, hasło, miesięczne opłaty abonamentowe, styl jazdy (profil kierowcy) opracowany – wygenerowany przez system na podstawie następujących parametrów: prędkości chwilowe, średnie, przyspieszenia, sposoby hamowania, chwilowe obroty silnika zużycia paliwa, sposób korzystania z hamulca, biegów itd.
Firma X pragnie zapewnić bezpieczne, niezawodne, ekologiczne środki transportu dla swoich pracowników, dla których podróże służbowe są częścią pracy. Przy doborze środków transportu firma kieruje się poziomem stanowiska służbowego, rodzajem wykonywanej pracy oraz funkcją, jaką spełnia samochód dla danego stanowiska.</td></tr>
</table>

<table>
<tr><td></td><td>Działania Firmy X nastawione są na zapewnienie bezpiecznej jazdy swoim pracownikom oraz na ochronę środowiska przez minimalizowanie negatywnego oddziaływania na otoczenie. Dlatego też Firma X zamierza wprowadzić system Ekojazda, który pozwala na stosowanie zasad ekologicznej eksploatacji pojazdów. Wdrożenie systemu ma na celu m.in. propagowanie odpowiednej postaw kierowców, monitorowanie, raportowanie sposobu eksploatacji pojazdów przez użytkowników.
Styl jazdy, ilość spalanego paliwa i emisji zanieczyszczeń są regularnie oceniane przez analityka wskazanego przez właściciela biznesowego. Jeżeli któryś z powyższych czynników jest poza zakresem norm, to właściciel biznesowy lub administrator systemu będą analizować czynniki wspólnie z użytkownikiem pojazdu oraz jego przełożonym. Jeżeli ustalone zmiany w stylu jazdy nie zostaną wdrożone, to kierowca pojazdu będzie obciążany kosztami ponadnormatywnego zużycia materiałów i pojazdu.
System Ekojazda dostarcza mała firma Start-up Sp. z o.o. z siedzibą w Poznaniu, która jako projekt start-up przygotowała sprzęt i oprogramowanie pozwalające wdrożyć system.
Firma Start-up dostarcza rozwiązanie oraz zapewnia wsparcie Firmie X i jest podmiotem przetwarzającym dane zgodnie z art. 28 RODO.
Wybór dostawcy rozwiązania był poprzedzony kilkumiesięczną analizą dostępnych na rynku rozwiązań. Decyzja o wyborze Start-up była spowodowana tym, że firma ta, jako podmiot przetwarzający, zapewnia oprócz nowoczesnego rozwiązania również wysoki standard ochrony danych osobowych.
Potwierdziły to liczne spotkania administratora z dostawcą rozwiązania, na których przedstawione zostały zasady działania systemu oraz wdrożone techniczne i organizacyjne środki bezpieczeństwa zapewniające odpowiedni do ryzyka poziom bezpieczeństwa (załącznik: „Start-up techniczne i organizacyjne środki.xlsx").
Start-up wyznaczył inspektora ochrony danych, który nadzoruje wypełnianie obowiązków wynikających z RODO.
Dostarczył również swoją Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym (załączniki: „PolitykaBezpieczenstwaEkojazda.pdf", „Plan ciągłości działania", „Certyfikat jakości urządzeń montowanych w samochodach") oraz zgodnie z art. 30 RODO prowadzi rejestr kategorii czynności przetwarzania.</td></tr>
<tr><td>4. Charakter przetwarzania</td><td>
<table>
<tr><th>Parametry charakteru przetwarzania</th><th>Tak / Nie</th></tr>
<tr><td>przetwarzane w sposób systematyczne i długoterminowo</td><td>Tak</td></tr>
<tr><td>przetwarzane w sposób systematyczne i krótkoterminowo</td><td></td></tr>
<tr><td>przetwarzane w sposób sporadycznie i długoterminowo</td><td></td></tr>
<tr><td>przetwarzane w sposób sporadycznie i krótkoterminowo</td><td></td></tr>
<tr><td>przetwarzane na dużą skalę</td><td>Tak</td></tr>
<tr><td>stosowana jest nowa lub złożona technologia</td><td>Tak</td></tr>
</table>
dane przetwarzane w sposób ciągły, długoterminowo, z zastosowaniem nowej technologii, wyłącznie w sposób elektroniczny
</td></tr>
</table>

3. Rekomendacje w celu minimalizacji wpływu na ochronę danych osobowych

Dla każdego potencjalnego ryzyka naruszenia prywatności należy określić możliwe środki zaradcze i działania, które je wyeliminują lub zmniejszą. Typowe rozwiązania obejmują zwykle:

- rezygnację z przetwarzania części danych osobowych;
- ograniczenie czasu przechowywania danych i zaplanowanie ich bezpiecznej likwidacji;
- wdrożenie odpowiednich technologii i organizacyjnych oraz fizycznych środków bezpieczeństwa;
- zastosowanie pseudonimizacji lub anonimizacji danych;
- przygotowanie instrukcji o sposobie używania nowego systemu i odpowiednie przeszkolenie pracowników;
- zapewnienie transparentności informacji podmiotom danych (jakie dane i w jaki sposób są przetwarzane);
- wybór dostawców oferujących większy poziom bezpieczeństwa;
- przeprowadzenie audytu u podmiotu przetwarzającego.

Na tym etapie dobierz adekwatne środki zaradcze, opierając się na ocenie skuteczności poszczególnych rozwiązań. Wybierz te, które są najkorzystniejsze dla podmiotów danych, projektu i administratora danych.

Tabela 6. Rekomendacje w celu zminimalizowania wpływu na prywatność na podstawie analizy ryzyka

NR-001	Przeprowadzenie oceny prawnie usprawiedliwionego interesu.
NR-002	1) Wprowadzenie zasady każdorazowej akceptacji regulaminu przez dział prawny i IOD. 2) Wdrożenie dodatkowych zabezpieczeń w systemie Ekojazda, które nie pozwolą na przetwarzanie danych i udział w konkursie bez akceptacji regulaminu. 3) Administrator każdorazowo przed rozpoczęciem konkursu przeprowadzą szeroką kampanię informacyjną dotyczącą konkursu, w tym również konsultacje indywidualne z AS.
NR-003	1) Dostosowanie i weryfikacja umowy powierzenia przetwarzania danych – wypełnienie checklisty: Art.28Powierzenie-checklista_end_Ekojazda.docx. 2) Ustalenie ze Start-up Sp. z o.o. SLA gwarantującego wyższy poziom dostępności systemu Ekojazda. 3) Gwarancja odpowiedniego poziomu wsparcia technicznego i przedstawienie Planu ciągłości działania dla systemu Ekojazda (załącznik X) przez Start-up.
NR-004	Ustalenie podstawy prawnej przetwarzania danych w państwie trzecim – Wielkiej Brytanii – np. zawarcie umowy oparte na standardowych klauzulach umownych.
NR-005	Dokonanie weryfikacji zakresu danych w ocenie prawnie usprawiedliwionego interesu mającej na celu ustalenie adekwatności danych do celu ich przetwarzania.

NR-006	1) Przeprowadzenie konsultacji w sprawie zrozumienia tekstu zapisów obowiązków informacyjnych z osobami, których obowiązek dotyczy, oraz na podstawie wniosków z konsultacji dostosowanie zapisów obowiązku informacyjnego. 2) Wprowadzenie dla pracowników możliwości indywidualnych konsultacji z AS. 3) Transparentne wytłumaczenie pracownikom, dlaczego prawo do sprzeciwu nie będzie realizowane. 4) Przygotowanie i spełnienie obowiązku informacyjnego w postaci: a) regulaminu pracy; b) wiadomości przesłanej e-mailem do wszystkich osób, których dane są przetwarzane w systemie Ekojazda; c) rozesłanie newslettera do wszystkich pracowników; d) wdrożenie i przekazanie pracownikom Polityki samochodowej w Firmie X Sp. z o.o.
NR-009	Zaleca się przeprowadzanie audytu przed rozpoczęciem przetwarzania danych przez firmę Start-up, weryfikującego stosowanie wskazanych w art. 28 RODO zasad przetwarzania danych oraz oceny technicznych i organizacyjnych środków bezpieczeństwa.
NR-010	Ustalenie zasad dotyczących długości i częstotliwości zmiany haseł.
NR-012	Ustalenie i wdrożenie zasady ujawniania i przekazywania danych na zewnątrz i wewnątrz organizacji.
NR-014	Transparentne poinformowanie pracowników o zakresie danych podlegających sprostowaniu, m.in. w obowiązku informacyjnym.
NR-017	Opracowanie zasad przekazywania informacji o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych w Firmie X.
NR-018	Ustalenie zasad przekazywania danych, w tym z geolokalizacji, które są przetwarzane w ramach konkursu na bezpieczną jazdę, gdzie podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. b (akceptacja regulaminu konkursu).
NR-019	Przeprowadzenie oceny prawnie usprawiedliwionego interesu.
NR-020	Przeprowadzenie oceny prawnie usprawiedliwionego interesu, w którym zweryfikowane zostaną zasady zautomatyzowanego podejmowania decyzji, w tym profilowania – w szczególności ustalenie, co będzie podstawą przetwarzania danych w tym procesie.
NR-022	Ustalenie przez AS zasady przetwarzania danych o karalności (zabranie prawa jazdy) oraz informacji o dłuższych chorobach.

4. Plan rekomendowanych działań

Dla każdego rekomendowanego środka zaradczego ograniczającego ryzyko należy określić konkretne działania, osobę odpowiedzialną i termin realizacji. Wszelkie decyzje dotyczące prywatności i wybranych działań powinny być odpowiednio udokumentowane i zaakceptowane. Zidentyfikowane działania są konieczne do uzyskania zgodności z RODO i stworzenia strategii ograniczenia ryzyka naruszenia prywatności.

W tej części raportu należy opisać, jakie działania są podejmowane (krótko lub długoterminowo) i jak będą monitorowane. Mogą być także linki do innych procesów, np. proponowane działanie może odnosić się do kontroli zabezpieczeń (takich jak zasady dostępu do systemu). To z kolei łączy się z procesami bezpieczeństwa w organizacji.

Złożone projekty często wymagają wielokrotnego przeglądu OSOD. W tej sekcji należy podać plan działań oraz wskazać przypadki, kiedy trzeba będzie dokonać ponownego przeglądu oceny.

Tabela 7. Plan działań

Numer referencyjny	Uzgodnione działanie	Osoba odpowiedzialna	Termin realizacji
D-001 (NR-001)	Przeprowadzenie oceny prawnie uzasadnionego interesu	właściciel biznesowy (przy współpracy z działem prawnym, IT oraz IOD)	dd.mm.rrrr
D-002 (NR-002)	Wdrożenie instrukcji obligującej właściciela biznesowego tego procesu do każdorazowej akceptacji regulaminu przez dział prawny i IOD przed uruchomieniem konkursów	dział prawny	dd.mm.rrrr
D-003 (NR-002)	Wdrożenie dodatkowych zabezpieczeń w systemie Ekojazda, które nie pozwolą na przetwarzanie danych i udział w konkursie bez akceptacji regulaminu	właściciel biznesowy oraz Start-up	dd.mm.rrrr
D-004 (NR-002)	Administrator przed rozpoczęciem konkursu każdorazowo przeprowadza szeroką kampanię informacyjną dotyczącą konkursu, w tym również konsultacje indywidualne z AS	właściciel biznesowy	dd.mm.rrrr
D-005 (NR-03)	Dostosowanie i weryfikacja umowy powierzenia przetwarzania danych – wypełnienie checklisty: Art.28Powierzenie-checklista_end_Ekojazda.docx	dział prawny (wsparcie IOD)	dd.mm.rrrr
D-006 (NR-03)	Ustalenie z firmą Start-up Sp. z o.o. SLA gwarantującego wyższy poziom dostępności systemu Ekojazda. Weryfikacja Planu ciągłości działania dla systemu Ekojazda	właściciel biznesowy (wsparcie IT i IOD)	dd.mm.rrrr
D-007 (NR-04)	Ustalenie podstawy prawnej przetwarzania danych w państwie trzecim – Wielkiej Brytanii	dział prawny (wsparcie IOD)	dd.mm.rrrr

Numer referencyjny	Uzgodnione działanie	Osoba odpowiedzialna	Termin realizacji
D-008 (NR-05)	Dokonanie weryfikacji zakresu danych przetwarzanych w systemie Ekojazda oraz ustalenie ostatecznego adekwatnego do celu zakresu danych	właściciel biznesowy (wsparcie IOD)	dd.mm.rrrr
D-009 (NR-06)	Przeprowadzenie konsultacji z osobami, których dane będą przetwarzane w systemie Ekojazda, i ustalenie wpływu przetwarzania danych na te osoby	właściciel biznesowy	dd.mm.rrrr
D-010 (NR-06)	Przeprowadzenie weryfikacji rozumienia zapisów obowiązku informacyjnych wśród osób, których obowiązek dotyczy, oraz dostosowanie zapisów obowiązku informacyjnego na podstawie wniosków z konsultacji	właściciel biznesowy (wsparcie IOD)	dd.mm.rrrr
D-011 (NR-06)	Wprowadzenie dla pracowników możliwości indywidualnych konsultacji z AS, w tym transparentne wytłumaczenie, dlaczego prawo do sprzeciwu nie będzie realizowane	właściciel biznesowy	dd.mm.rrrr
D-012 (NR-06)	Wdrożenie i przekazanie pracownikom Polityki samochodowej w Firmie X Sp. z o.o.	właściciel biznesowy	dd.mm.rrrr
D-013 (NR-06)	Przygotowanie i spełnienie obowiązku informacyjnego w: • regulaminie pracy, • wiadomości przesłanej e-mailem do wszystkich osób, których dane są przetwarzane w systemie Ekojazda, • przesłanie newslettera do wszystkich pracowników	dział prawny przy wsparciu IOD	dd.mm.rrrr
D-014 (NR-09)	Przeprowadzanie audytu u podmiotu przetwarzającego w firmie Start-up, weryfikującego stosowanie wskazanych w art. 28 RODO zasad przetwarzania danych oraz oceny technicznych i organizacyjnych środków bezpieczeństwa	IOD i IT	dd.mm.rrrr
D-015 (NR-010)	Ustalenie i wdrożenie zasad dotyczących długości i częstotliwości zmiany haseł na telefonach komórkowych i tabletach	dział IT (wsparcie IOD)	dd.mm.rrrr
D-016 (NR-010)	Uaktualnienie IZSI o stosowaniu zasad dotyczących długości haseł i dodatkowego bezpieczeństwa urządzeń mobilnych, które mają dostęp do aplikacji systemu Ekojazda	dział IT (wsparcie IOD)	dd.mm.rrrr
D-017 (NR-012)	Wdrożenie procedury ujawniania i przekazywania danych na zewnątrz i wewnątrz firmy	właściciel biznesowy (wsparcie IOD)	dd.mm.rrrr

Książka omawia wszystkie aspekty oceny ryzyka ujętego w RODO, w tym fazę projektowania, ocenę skutków i przypadek incydentu bezpieczeństwa.

W pierwszej części publikacji przedstawiono mechanizm oceny ryzyka i wątpliwości interpretacyjne, które się z nim łączą. Uwzględniono orzecznictwo oraz wytyczne wyrażone w stanowiskach organów nadzorczych (w tym polskiego organu). Kwestie sporne zostały omówione na przykładach przeprowadzonych analiz ryzyka (np. przez administratorów z sektora publicznego), a także wytycznych opublikowanych m.in. przez organy nadzorcze.

W drugiej części książki za pomocą praktycznych przykładów przedstawiono różne sposoby oceny ryzyka. W każdym z nich autorzy prowadzą czytelnika krok po kroku przez cały proces analizy ryzyka, m.in. za pomocą list kontrolnych.

Autorzy zadbali o to, aby ocena ryzyka mieściła się w kryteriach wynikających z RODO, a jednocześnie była rozliczalna, czyli na przykład, aby można było prześledzić i zrozumieć, dlaczego został zdefiniowany konkretny poziom ryzyka oraz z jakiego powodu przyjęto takie, a nie inne metody jego minimalizacji.

Zamieszczone w publikacji praktyczne przykłady dotyczą m.in.:
- przechowywania dokumentacji medycznej,
- rezerwacji wizyty lekarskiej za pomocą chatbota,
- procesu rekrutacji,
- pracy zdalnej.

„Tego typu publikacji do tej pory na rynku prawniczym i rynku ochrony danych osobowych nie było. Jest to książka o bardzo praktycznym wymiarze, która z pewnością będzie bardzo szeroko wykorzystywana (…)".
Dr hab. Agnieszka Grzelak, prof. ALK

Mirosław Gumularz – doktor nauk prawych; radca prawny (GKK Gumularz Kozik), adiunkt w Wyższej Szkole Bankowej w Warszawie. Jako doradca społeczny ds. ochrony danych osobowych w Ministerstwie Cyfryzacji brał udział w pracach nad wdrożeniem RODO do polskiego porządku prawnego. Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg normy ISO 27001 (zarządzanie bezpieczeństwem), a także normy ISO/IEC 27701:2019 (zarządzanie prywatnością). Autor lub współautor licznych publikacji z zakresu ochrony danych osobowych oraz nowych technologii.

Tomasz Izydorczyk – inżynier, doradca w zakresie organizacji i zarządzania w sektorze prywatnym oraz w administracji publicznej. Specjalizuje się w prawnej i organizacyjnej ochronie danych osobowych. Jest wykładowcą m.in. w Wyższej Szkole Bankowej w Poznaniu, w Wyższej Szkole Bankowej w Warszawie i na Uniwersytecie Wrocławskim. Współautor wielu publikacji z zakresu ochrony danych osobowych. Członek zarządu SABI – Stowarzyszenia Inspektorów Ochrony Danych. Certyfikowany audytor wiodący ISO/IEC 27001 oraz audytor ISO/IEC 27701.

9788382235333 W01P01

ISBN 978-83-8223-533-3
9 788382 235333

ZAMÓWIENIA:
INFOLINIA 801 04 45 45
ZAMOWIENIA@WOLTERSKLUWER.PL
WWW.PROFINFO.PL

CENA 119 ZŁ (W TYM 5% VAT)