ŚLĄSKI ZWIĄZEK GMIN I POWIATÓW
40-048 Katowice, ul. Tadeusza Kościuszki 43/5
tel. +48 32 25 11 021, 25 11 241
www. silesia.org.pl, email: zwiazek@silesia.org.pl
NIP: 634 10 87 850, Konto ING Bank Śląski 03 1050 1214 1000 0007 0001 3261

Katowice, dnia 22 grudnia 2021 roku

Rekomendacja 2/21

Komisja ds. Ochrony Danych Osobowych

Śląskiego Związku Gmin i Powiatów z siedzibą w Katowicach

dotyczy: wykonywania sprawdzeń przez Inspektora ochrony danych w zakresie zgodności przetwarzania danych osobowych z przepisami oraz polityk administratora (lub podmiotu przetwarzającego).

W celu wypracowania wspólnego stanowiska i jednolitego postępowania gmin i powiatów zrzeszonych w Śląskim Związku Gmin i Powiatów z siedzibą w Katowicach w zakresie stosowania przepisów o ochronie danych osobowych w związku z monitorowaniem przestrzegania przepisów rozporządzenia 2016/679 (RODO) wskazuje się, jak poniżej.

A. KONTEKST NORMATYWNY

Komisja ds. Ochrony Danych Osobowych (zwana dalej Komisją) podjęła inicjatywę przygotowania rekomendacji zawierającej podstawowe wskazania w zakresie bezpieczeństwa przetwarzania danych osobowych, dotyczącej sprawdzeń wykonywanych przez Inspektora ochrony danych.

I. Przepisy prawa merytorycznego

Zgodnie z art. 39 ust. 1 lit. a oraz art. 39 ust. 1 lit. b RODO w związku z art. 38, Inspektor ochrony danych ma obowiązek monitorować przestrzeganie przepisów RODO i innych przepisów dotyczących ochrony danych osobowych. W związku z tym należy zapewnić, że Inspektor wykonuje to zadanie oraz zadbać o właściwe udokumentowanie tych działań.

II. Definicje

1. **Dane osobowe**

   Zgodnie z art. 4 pkt 1 RODO dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą") przy czym możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

2. **Przetwarzanie**

   Zgodnie z art. 4 pkt 2 RODO przetwarzanie danych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób

zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Każdy rodzaj operacji na danych musi posiadać swe wyraźne uzasadnienie, a ich wykonywanie powinno być ograniczone co do zakresu przetwarzania danych osobowych, formy przetwarzania, jak i czasu ich trwania.

3. **Sprawdzenie (audyty)**

Forma monitorowania, czynność mająca na celu zweryfikowanie zgodności przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz politykami wewnętrznymi administratora danych.

B. REKOMENDACJA

Celem niniejszej rekomendacji jest wskazanie możliwych do zastosowania rozwiązań z zakresu ochrony prywatności i przetwarzania danych osobowych w celu skutecznego monitorowania stosowania przepisów w ramach czynności przetwarzania realizowanych przez administratora lub podmiot przetwarzający.

Komisja ds. Ochrony Danych Osobowych przy Śląskim Związku Gmin i Powiatów rekomenduje w tym celu wykonywanie sprawdzeń realizowanych okresowo przez Inspektorów ochrony danych, w zakresie stosowania przepisów RODO i innych przepisów o ochronie danych osobowych oraz polityk administratora lub podmiotu przetwarzającego w zakresie ochrony danych osobowych.

Niniejsza rekomendacja dotyczy następujących aspektów stosowania monitorowania zgodności z przepisami poprzez wykonywanie sprawdzeń oraz dokumentowania tych czynności w następujących zakresach:

1. Cel sprawdzenia;
2. Rodzaj sprawdzenia;
3. Plan sprawdzenia;
4. Wykonanie sprawdzenia;
5. Przygotowanie sprawozdania;
6. Rekomendacje Inspektora ochrony danych w zakresach objętych sprawdzeniem;
7. Przekazanie sprawozdania;
8. Monitorowanie wdrożenia rekomendacji przyjętych do stosowania.

W celu należytego monitorowania stosowania przepisów, Inspektor ochrony danych przygotowuje dokumentację i przedstawia ją administratorowi danych. Sposób przygotowania dokumentacji, terminy jej opracowywania oraz obieg dokumentów powinien zostać ujęty w dokumentacji systemu ochrony danych

osobowych, na przykład w wewnętrznych politykach administratora danych osobowych lub podmiotu przetwarzającego.

1. **Cel sprawdzenia**

Celem sprawdzenia jest ustalenie i udokumentowanie w sprawozdaniu stanu faktycznego, na podstawie którego następuje ocena przestrzegania przepisów z zakresu ochrony danych osobowych pod kątem oceny techniczno-organizacyjnych zasad stosowanych u administratora lub podmiotu przetwarzającego oraz faktycznej realizacji czynności przetwarzania. W związku z tym, sprawdzenie polega na przeprowadzeniu przez Inspektora ochrony danych czynności, dzięki którym jest ustalany ów stan faktyczny w zakresie przetwarzania danych osobowych i spełnienia prawnych obowiązków ochrony danych osobowych. Inspektor wykonując sprawdzenie winien zbadać zgodność procesu przetwarzania z zasadami określonymi w art. 5 RODO, pozostałymi postanowieniami RODO, wymogami innych przepisów prawa, jeśli swoim zakresem materialnym przedmiotowego procesu dotyczą, wewnętrznymi politykami przyjętymi przez administratora lub podmiot przetwarzający oraz z zaleceniami w zakresie oceny skutków dla ochrony danych osobowych, w tym wydanymi przez Prezesa Urzędu Ochrony Danych Osobowych w ramach uprzednich konsultacji.

Czynności te powinny być dokumentowane. W sprawozdaniu Inspektor ochrony danych zajmuje stanowisko określając czy stosowane zasady ochrony są wystarczające, czy nie doszło do naruszenia lub istnieje potencjalne ryzyko naruszenia ochrony danych.

2. **Rodzaje sprawdzeń**

Komisja rekomenduje przyjęcie dwóch rodzajów sprawdzeń:

1) **Sprawdzenia planowe** – planowane od początku roku sprawozdawczego i ściśle wykonywane wg planu, z zachowaniem obszarów objętych sprawdzeniem oraz terminów wykonania i wydatku czasu poświęconego na sprawdzenie;

2) **Sprawdzenie doraźne** – wykonywane w związku z zaistnieniem incydentu lub wynikające z podejrzenia Inspektora ochrony danych dotyczącego potencjalnego zagrożenia dla ochrony danych. Sprawdzenia doraźne mogą być inicjowane przez Inspektora ochrony danych lub zlecane przez administratora (lub podmiot przetwarzający) w ramach wspierania i doradztwa wykonywanego przez Inspektora ochrony danych. Sprawdzenia doraźne mogą być również wykonywane na uzasadniony wniosek innych osób np. pracowników upoważnionych do przetwarzania danych osobowych, podmiotów danych osobowych, pracowników podmiotów zewnętrznych współpracujących z administratorem (lub z podmiotem przetwarzającym). Sprawdzeniem doraźnym można objąć także weryfikację stosowania przyjętych przez administratora (lub podmiot przetwarzający) środków organizacyjnych zapewniających ochronę danych osobowych.

3. Planowanie wykonania sprawdzenia.

Komisja rekomenduje przygotowanie planu sprawdzeń na cały rok z góry. Przygotowanie planu sprawdzenia ma na celu zapoznanie administratora z planowanym zakresem, terminami i czasem wykonania sprawdzeń. Opracowanie planu sprawdzeń pozwala na ustalenie z administratorem terminów wykonania sprawdzenia pozwalające na wykluczenie sytuacji ewentualnej kolizji terminów sprawdzeń z realizacją ważnych zadań administratora lub podmiotu przetwarzającego. Plan sprawdzenia Inspektor wykonuje na koniec roku poprzedzającego i przedstawia do wiadomości administratora w terminie, który powinien zostać określony w politykach administratora lub podmiotu przetwarzającego. Komisja rekomenduje ustalenie w politykach bezpieczeństwa administratora lub podmiotu przetwarzającego konkretnego terminu, w którym Inspektor przedstawia plan sprawdzeń na rok następny. Komisja zwraca uwagę, że opracowanie planu sprawdzeń nie wynika z przepisów prawa regulujących wykonywanie funkcji Inspektora i nie jest obowiązkowe, aczkolwiek wykonanie planu może być pomocne zarówno dla Inspektora ochrony danych jak i administratora lub podmiotu przetwarzającego.

Sposób przekazania planu sprawdzeń powinien zostać uregulowany w politykach administratora. Plan może zostać przekazany bezpośrednio administratorowi lub za pośrednictwem wyznaczonego pracownika. Ze względu na zapis art. 38 ust. 3 RODO plan sprawdzenia nie musi być zatwierdzany przez administratora lub podmiot przetwarzający.

Plan powinien zawierać co najmniej następujące informacje:

1) Wyszczególnienie obszarów planowanych do sprawdzenia.
2) Orientacyjny termin rozpoczęcia sprawdzenia.
3) Dodatkowo plan może zawierać:
   a) wyszczególnienie osób zaangażowanych w wykonanie sprawdzenia,
   b) wyszczególnienie lokalizacji gdzie będzie się odbywało sprawdzenie.

Komisja wskazuje, że w politykach administratora powinien być ustalony sposób przekazania sprawozdania.

Sprawdzenie doraźne jest wykonywane poza planem sprawdzeń. Sprawdzenie takie może nastąpić w wyniku wystąpienia naruszenia ochrony danych, incydentu, który w konsekwencji może doprowadzić do naruszenia lub istnieje uzasadnione podejrzenie takich konsekwencji. Inspektor ochrony danych może przeprowadzić sprawdzenie doraźne również w sytuacji gdy uzna, że konieczne jest dokonanie takiego sprawdzenia w obszarze nie objętym planem sprawdzeń lub na wyraźne zlecenie administratora danych lub podmiotu przetwarzającego.

4. Wykonanie sprawdzenia

Każdy rodzaj sprawdzenia składa się z następujących etapów czynności Inspektora ochrony danych:

1) Działania przygotowawcze

Przed rozpoczęciem sprawdzenia Inspektor ochrony danych podejmuje czynności mające na celu przygotowanie go oraz osób reprezentujących administratora lub podmiot przetwarzający podczas sprawdzenia. Komisja rekomenduje aby w ramach tych działań Inspektor poinformował osoby, które będą uczestniczyły w sprawdzeniu, o:

a) terminie rozpoczęcia czynności sprawdzających,

b) zakresie dokumentacji, które osoba uczestnicząca powinna przygotować do sprawdzenia,

c) planowanym terminie zakończenia sprawdzenia,

d) sposobie uzgadniania wyników sprawdzenia,

e) ewentualnych innych uzasadnionych wymaganiach wobec sprawdzanego na przykład w zakresie udostępnienia pomieszczenia, oględzin urządzeń itp.

Komisja rekomenduje aby Inspektor odpowiednio wcześnie informował osoby uczestniczące w sprawdzeniu biorąc pod uwagę zakres sprawdzenia i zadania administratora lub podmiotu przetwarzającego realizowane przez osoby uczestniczące w sprawdzeniu. Przy sprawdzeniu doraźnym ww. osoby nie są informowane.

Komisja zwraca uwagę, że informowanie opisane w niniejszym podpunkcie osób uczestniczących w sprawdzeniu, w określonych przypadkach może zostać pominięte.

Komisja rekomenduje, aby we właściwych politykach bezpieczeństwa uregulować możliwość przebywania Inspektora ochrony danych w budynkach i pomieszczeniach administratora lub podmiotu przetwarzającego poza godzinami funkcjonowania jednostki organizacyjnej.

2) Czynności Inspektora ochrony danych -faktyczne sprawdzenie

Sprawdzenie wykonywane przez Inspektora ochrony danych powinno być wykonywane sprawnie, bez zbędnego zaskakiwania osób uczestniczących w czynnościach, a przede wszystkim, w sposób niezakłócający pracy administratora lub podmiotu przetwarzającego. Komisja zwraca uwagę, że administrator lub podmiot przetwarzający powinni dołożyć wszelkich starań, aby osoby odpowiedzialne za przetwarzanie danych, których dotyczy sprawdzenie wzięły udział w sprawdzeniu, nie zatajały informacji lub nie podawały informacji nieprawdziwych oraz aktywnie wspierały Inspektora ochrony danych w wykonaniu czynności sprawdzających.

W celu rzetelnego i prawidłowego wykonania sprawdzenia, Komisja zaleca, aby administrator lub podmiot przetwarzający zapewnił Inspektorowi ochrony danych:

a) wstęp w trakcie i po zakończeniu dnia pracy na grunt oraz do budynków, lokali lub innych pomieszczeń;

b) wgląd do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym sprawdzenia;

c) możliwość przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;

d) możliwość zlecania komórkom organizacyjnym funkcjonującym u administratora (lub w podmiocie przetwarzającym), w tym w szczególności działowi prawnemu i IT, sporządzania ekspertyz i opinii,

e) dokumentowanie czynności wykonanych przez Inspektora ochrony danych w tym gromadzenie materiału dowodowego.

Istotą sprawdzenia pozostaje uzyskanie przez Inspektora ochrony danych informacji na temat przetwarzania danych osobowych oraz wykonania prawnych obowiązków administratora lub podmiotu przetwarzającego w zakresie ochrony danych osobowych, które pozwolą na zweryfikowanie zgodności przetwarzania danych z przepisami o ochronie danych osobowych oraz politykami administratora lub podmiotu przetwarzającego. Komisja rekomenduje przyjąć zasadę, że Inspektor ochrony danych przeprowadza czynności w takim zakresie, jaki jest mu wystarczający do oceny zgodności przetwarzania danych osobowych z przepisami i w dalszym etapie na opracowanie sprawozdania. W celu uzyskania informacji oraz udokumentowania wniosków i rekomendacji ze sprawdzenia, Inspektor gromadzi materiał dowodowy w wyniku:

a) Odebrania ustnych lub pisemnych wyjaśnień – poprzez sporządzanie notatki lub odebranie pisemnego oświadczenia;

b) Przeprowadzania oględzin;

c) Dostępu do urządzeń, nośników oraz systemów informatycznych służących lub wspomagających przetwarzanie danych osobowych w tym celu może wykonywać dokumentację fotograficzną, gromadzić wydruki lub kopie obrazu wyświetlonego na ekranie urządzenia;

d) Wykonywania kopii dokumentów.

Komisja zwraca uwagę, że w przypadku wykonywania czynności sprawdzających w zakresie systemów informatycznych, jeśli Inspektor ochrony danych nie jest w stanie samodzielnie udokumentować stanu faktycznego, może zwrócić się do administratora systemu informatycznego lub innej osoby, która takiego dowodu może dostarczyć, o wykonanie określonych czynności w systemie pozwalających na takie udokumentowanie. Administrator lub podmiot przetwarzający powinien zapewnić, że osoby te mają obowiązek współpracować z Inspektorem ochrony danych w tym zakresie.

Dokumentacja ze sprawdzenia może mieć formę tradycyjną lub elektroniczną wedle uznania Inspektora ochrony danych. Komisja rekomenduje gromadzenie dowodów w postaci elektronicznej.

Wszelka dokumentacja zebrana podczas sprawdzenia tworzy akta sprawdzenia, które przechowuje Inspektor ochrony danych.

5. Przygotowanie sprawozdania ze sprawdzenia.

Po przeprowadzeniu czynności sprawdzających Inspektor ochrony danych przystępuje do opracowania sprawozdania.

Celem opracowania sprawozdania jest :

1) Podsumowanie czynności wykonanych podczas sprawdzenia.
2) Dokonanie oceny w oparciu o zebrany materiał dowodowy czy realizowane czynności są zgodne z prawem i czy nie zachodzi możliwość powstania ryzyka naruszenia ochrony.
3) Zaproponowanie administratorowi lub podmiotowi przetwarzającemu rekomendacji mających na celu:
   a) Wskazanie działań podnoszących bezpieczeństwo przetwarzania danych osobowych;
   b) W przypadku wykrycia potencjalnych sytuacji prowadzących do naruszenia ochrony wskazanie działań, które pozwolą na przywrócenie stanu prawidłowego.
4) Sprawozdanie powinno zawierać następujące elementy:
   a) Podstawę wykonania sprawdzenia (plan sprawdzenia, spostrzeżenie, zlecenie);
   b) Opis sposobu przeprowadzenia sprawdzenia i gromadzenia dowodów;
   c) Opis stanu faktycznego stwierdzonego podczas sprawdzenia oraz wszelkie inne informacje mające znaczenie dla oceny zgodności przetwarzania z przepisami w tym zakresie oraz politykami administratora lub podmiotu przetwarzającego;
   d) Stwierdzenie czy w badanym zakresie nie doszło do naruszeń ochrony lub istnieje potencjalne ryzyko naruszenia ochrony, czy nie doszło do złamania ustalonych zasad przetwarzania administratora lub podmiotu przetwarzającego określonego w politykach; czy stosowane zasady ochrony są wystarczające,
   e) Rekomendacje i wnioski Inspektora ochrony danych.

Sprawozdanie przed przekazaniem administratorowi lub podmiotowi przetwarzającemu, powinno zostać zweryfikowane przez osoby uczestniczące w sprawdzeniu w zakresach, za które były odpowiedzialne. W przypadku wniesienia uwag, Inspektor ochrony danych uwzględnia je w sprawozdaniu lub umieszcza adnotację o braku akceptacji konkretnych zapisów lub propozycje zapisów zgłoszone przez osoby uczestniczące w sprawdzeniu, które nie zostały zaakceptowane przez Inspektora ochrony danych.

Dokumentacja sprawozdania może mieć postać tradycyjną lub elektroniczną. W przypadku dokumentacji elektronicznej, sprawozdanie powinno mieć formę uniemożliwiającą modyfikację dokumentu lub pozwalającą na stwierdzenie każdej modyfikacji. Rekomenduje się, że w przypadku

dokumentacji tradycyjnej (papierowej) Inspektor ochrony danych powinien zaparafować każdą stronę sprawozdania.

6. **Rekomendacje i wnioski inspektora**

   Inspektor ochrony danych w sprawozdaniu, w przypadku zauważenia niezgodności pomiędzy stanem wymaganym prawem a realizacją w badanym obszarze, powinien przedstawić propozycje działań mających na celu poprawę stanu zastanego.

7. **Przekazanie sprawozdania.**

   Sposób przekazania sprawozdania administratorowi (lub podmiotowi przetwarzającemu) powinien zostać uregulowany w politykach dotyczących bezpieczeństwa przetwarzania danych osobowych. Po przekazaniu sprawozdania administrator lub podmiot przetwarzający może ustosunkować się do zaproponowanych przez Inspektora rekomendacji.

8. **Monitorowanie wdrożenia rekomendacji przyjętych do stosowania.**

   1) Monitorowanie realizacji rekomendacji przyjętych do wprowadzenia może zostać ujęte w planach sprawdzeń na następne okresy;

   2) W uzasadnionych przypadkach tj. np. gdy podczas sprawdzenia byłyby wykryte uchybienia w procesie przetwarzania danych lub zabezpieczenia danych osobowych wymagające natychmiastowej reakcji i poprawy Inspektor ochrony danych i kierujący sprawdzanym obszarem mogą monitorować wdrożenie rekomendacji w ustalonym przez nich terminie.

Przy wypracowaniu stanowiska wzięto pod uwagę przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).