Zarządzenie nr 3/10/2021
Burmistrza Miasta i Gminy Ryn
z dnia 20 października 2021 roku

w sprawie wprowadzenia „Regulaminu dla pracowników dotyczącego przetwarzania danych osobowych”

Na podstawie 31 Ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2021 roku, poz. 1372 z późń. zm.) oraz art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony danych osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1) zarządzam, co następuje:

§1

Wprowadzam „Regulamin dla pracowników dotyczący przetwarzania danych osobowych” stanowiący załącznik do niniejszego Zarządzenia.

§2

Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

§3

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy Ryn
Jarosław Filipek

Załącznik
do Zarządzenia nr 3/10/2021
Burmistrza Miasta i Gminy Ryn
z dnia 20 października 2021 roku

Regulamin dla pracowników dotyczący przetwarzania danych osobowych

Ryn, październik 2021 r.

Każdy pracownik, stażysta, praktykant jednostki odpowiada za bezpieczeństwo i przetwarzanie danych osobowych.

§ 1 Oznaczenie informacji

Osoby posiadające upoważnienie oraz mające dostęp do danych osobowych oraz informacji w związku z zajmowanym stanowiskiem lub pełnioną funkcją, samodzielnie klasyfikują dane osobowe, a w przypadku danych szczególnych lub informacji chronionej mają obowiązek stosować zapisy niniejszego dokumentu. Każda osoba posiadająca upoważnienie nadane przed Administratora ma obowiązek w codziennej pracy uwzględniać zakres nadanego upoważnienia, w przypadku kiedy zadania wynikające ze stosunku pracy są rozbieżne z nadanym upoważnieniem osoba ma obowiązek niezwłocznie wystąpić do Administratora o zmodyfikowanie upoważnienia.

§ 2 Inspektor Ochrony Danych

Administrator powołuje Inspektora Ochrony Danych (dalej jako IOD). IOD jest odpowiedzialny za prowadzenie całokształtu spraw związanych przetwarzaniem danych osobowych zgodnie z art. 39 RODO. Z IOD należy kontaktować się w każdej sprawie związanej z ochroną danych osobowych. Kontakt do IOD – rodo@miastoryn.pl

§ 3 Podstawy przetwarzania danych osobowych

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy zostanie spełniona jedna z przesłanek wynikająca z art. 6 RODO.
Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX RODO. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

W przypadku szczególnej kategorii danych przetwarzanie jest dopuszczalne tylko wtedy, gdy zostanie spełniona jedna z przesłanek określonych w art. 9 ust 2 i 3 RODO.

§ 4 Obowiązek informacyjny przy przetwarzaniu danych oraz powierzenie danych

Administrator podczas pozyskiwania danych osobowych od osoby, której dane dotyczą spełnia wobec niej obowiązek informacyjny zgodnie z art. 13 ust. 1 i 2 RODO.

W przypadku zbierania danych nie od osoby, której te dane dotyczą, osobę tą należy dodatkowo poinformować o źródle danych oraz uprawnieniach. W związku z tym administrator wobec tej osoby spełnia obowiązek administracyjny zgodnie z art. 14 ust. 1 i 2 RODO.

Klauzule informacyjne dołączamy do wszystkich pism np. wnioski, decyzje, zawiadomienia. Podczas fazy projektowania pism bardzo ważny jest kontakt z IOD, który opatrzy dane pismo odpowiednią klauzulą informacyjną, a wzór umowy odpowiednimi zapisami dotyczącymi powierzenia danych.

§ 5 Procedura realizacji praw osób, których dane dotyczą

Każda osoba, której dane dotyczą, jest uprawniona do wniesienia żądania do Administratora o zrealizowanie praw, o których mowa w art. 15 – 21 RODO, tj.:

a. prawo dostępu do danych,
b. prawo do sprostowania danych,
c. prawo do usunięcia danych („prawo do bycia zapomnianym"),
d. prawo do ograniczenia przetwarzania,
e. prawo do przenoszenia danych,
f. prawo do sprzeciwu wobec przetwarzania danych osobowych.

Prawo dostępu do danych przysługujące osobie, której dane dotyczą

Osoba, której dane dotyczą, ma prawo uzyskać od Administratora informację, czy przetwarza on dane osobowe jej dotyczące, a w przypadku zaistnienia takiego przetwarzania osoba ta ma prawo dostępu do swoich danych oraz uzyskania informacji o:

a. celach przetwarzania,
b. kategoriach odnośnych danych osobowych,
c. odbiorcach lub kategoriach odbiorców, którym zostaną lub zostały ujawnione dane osobowe,
d. planowanym okresie przechowywania danych osobowych, a sytuacji braku takiej możliwości – o kryteriach ustalania tego okresu,
e. prawie do sprostowania danych, usunięcia danych lub ograniczenia przetwarzania oraz prawie do wniesienia sprzeciwu wobec przetwarzania,
f. prawie do wniesienia skargi do organu nadzorczego,
g. źródle danych, jeśli dane pochodzą z innego źródła niż od osoby, której dane dotyczą,
h. zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, a także znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,
i. odpowiednich zabezpieczeniach związanych z przekazaniem, jeśli dane są przekazywane do państwa trzeciego lub organizacji międzynarodowej.

Administrator dostarcza osobie, której dane dotyczą, kopię posiadanych danych osobowych podlegających przetwarzaniu. Za każdą kolejną kopię danych osobowych Administrator może pobrać opłatę w wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie wskaże inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.
Prawo do uzyskania kopii, o której mowa w zdaniu poprzednim, nie może niekorzystnie wpływać na prawa i wolności innych osób.

Prawo do sprostowania danych

Osoba, której dane dotyczą może wnieść do Administratora żądanie niezwłocznego sprostowania danych jej dotyczących, jeśli stwierdzi, że dane są nieprawidłowe.
Osoba, której dane dotyczą może także wnieść (np. w formie dodatkowego oświadczenia) żądanie uzupełnienia danych, jeśli uzna, że są niekompletne.
Administrator informuje o sprostowaniu każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Prawo do usunięcia danych („prawo do bycia zapomnianym")

Osoba, której dane dotyczą ma prawo wniesienia do Administratora żądania niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator jest zobowiązany usunąć dane osobowe bez zbędnej zwłoki, jeśli zachodzi jedna z następujących okoliczności:

a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,

b. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
c. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania,
d. dane osobowe były przetwarzane niezgodnie z prawem,
e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega Administrator;
f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.

Jeśli Administrator upublicznił dane osobowe osoby wnoszącej o usunięcie danych i ma on obowiązek ich usunięcia, to uwzględniając dostępną technologię oraz koszt realizacji – podejmuje działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o fakcie, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych lub ich replikacje.

Prawo do usunięcia danych, zgodnie z art. 17 ust. 3 RODO, nie ma zastosowania w zakresie, w jakim przetwarzanie jest niezbędne:
a. do korzystania z prawa do wolności wypowiedzi i informacji,
b. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
c. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) RODO i art. 9 ust. 3 RODO,
d. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że realizacja prawa do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania,
e. do ustalenia, dochodzenia lub obrony roszczeń.

Administrator informuje o usunięciu danych każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą może wnieść do Administratora żądanie o ograniczenie przetwarzania dotyczących jej danych osobowych w następujących przypadkach:
a. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych,
b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
c. administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
d. osoba, której dane dotyczą, wniosła na mocy art. 21 ust. 1 RODO sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Jeżeli przetwarzanie zostało ograniczone to dane osobowe można przetwarzać, z wyjątkiem przechowywania:
– wyłącznie za zgodą osoby, której dane dotyczą,
– w celu ustalenia, dochodzenia lub obrony roszczeń,
– w celu ochrony praw innej osoby fizycznej lub prawnej,
– z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.
Administrator informuje o ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Prawo do przenoszenia danych

Osoba, której dane dotyczą, jest uprawniona do wniesienia żądania przeniesienia danych jej dotyczących.
Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora, jeżeli:

a. przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych osobowych w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO oraz
b. przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
Wykonanie prawa do przeniesienia danych nie wyklucza wniesienia żądania o usunięcie danych osobowych.
Prawo do przeniesienia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
Prawo do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych osób.

Prawo do sprzeciwu

Osoba, której dane dotyczą, może w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, jeśli przetwarzanie jest oparte na art. 6 ust. 1 lit. e) RODO (przetwarzanie w interesie publicznym lub w ramach sprawowania władzy publicznej) lub art. 6 ust. 1 lit. f) RODO (prawnie uzasadnione interesy realizowane przez administratora), w tym profilowania na podstawie tych przepisów.
Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

§ 6 Udostępnianie danych osobowych

Administrator udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania, po weryfikacji ich tożsamości.

Dane osobowe mogą być udostępniane w następujących przypadkach:

1) na wniosek od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów prawa;
2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
3) na podstawie wniosku osoby, której dane dotyczą.

Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania, po weryfikacji podmiotu ubiegającego się o dostęp do danych osobowych.

W przypadku wątpliwości co do możliwości udostepnienia danych osobowych podmiotom zewnętrznym konieczne są konsultacje z IOD. Ostateczną decyzję o udostępnieniu danych podejmuje Administrator.

§ 7 Zasady dokonywania anonimizacji danych osobowych w dokumentach publikowanych w Biuletynie Informacji Publicznej

1) Pracownik przygotowujący dokument zawierający dane osobowe podlegające ujawnieniu w szczególności, sporządzający protokoły z posiedzeń rady, komisji, uchwały i inne dokumenty, które mają zostać umieszczone w Biuletynie Informacji Publicznej zobowiązany jest do wstępnej oceny przedmiotowego dokumentu pod względem dopuszczalności publikacji danych osobowych osób fizycznych nie pełniących funkcji publicznych lub kierowniczych.
2) W sytuacji stwierdzenia obecności danych osobowych osób fizycznych, uwzględniając definicję danych osobowych zawartych w art. 4 pkt. 1 RODO oraz szczególnej kategorii danych uwzględnionych w art. 9 ust. 1 RODO. Pracownik zobowiązany jest do dokonania analizy legalności publikacji danych osobowych w przedmiotowym dokumencie oraz dokonania anonimizacji zawartych w nich danych osobowych osób fizycznych tj. imion, nazwisk, adresu, nr PESEL, wieku, numeru telefonu, stanu zdrowia itp.
3) Pracownik odpowiedzialny za publikację ww. dokumentów w Biuletynie Informacji Publicznej lub stronach internetowych urzędu, zobowiązany jest do weryfikacji poprawności dokonanej anonimizacji danych osobowych w tych dokumentach.

§ 8 Środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzania danych osobowych

W godzinach pracy, zobowiązuje się pracowników do:

a) zwracania szczególnej uwagi na zachowanie osób wchodzących i wychodzących z siedziby jednostki;
b) reagowania na wejście do budynku i przebywanie w nim osób będących pod wpływem alkoholu lub innych środków odurzających;
c) reagowania na próby niszczenia, wynoszenia lub wywożenia mienia z budynku jednostki;
d) reagowania na próby wnoszenia do budynku przedmiotów niebezpiecznych, materiałów lub substancji budzących podejrzenie itp.;
e) natychmiastowego reagowania poprzez powiadomienie odpowiednich służb (Policja, Straż Pożarna, Pogotowie Ratunkowe) o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia mienia.

Administrator wyznacza pracowników, którzy są upoważnieni do otwierania głównych drzwi wejściowych do budynku oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy jednostki.

Pracownik, któremu zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązany jest do:

a) wykorzystywania ich zgodnie z przeznaczeniem,
b) nie kopiowania powierzonych kluczy bez zgody Administratora oraz udostępniania osobom trzecim,
c) nie udostępniania kodu cyfrowego do systemu alarmowego osobom trzecim.

Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, dokumentacji i innego wyposażenia.

W przypadku stwierdzenia nieprawidłowości lub naruszenia stanu zabezpieczeń, o których mowa powyżej, pracownik, który to stwierdził, niezwłocznie zgłasza incydent naruszenia danych osobowych.

Od momentu pobrania kluczy do momentu ich zdania na pracownikach urzędujących w tych pomieszczeniach spoczywa pełna odpowiedzialność za ich zabezpieczenie.

Po zakończeniu pracy pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających na:

a) zabezpieczeniu dokumentacji i pieczęci urzędowych;
b) zabezpieczeniu komputerów i nośników informacji;
c) wyłączeniu wszystkich urządzeń energetycznych zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp;
d) zamknięciu okien i drzwi;
e) pozostawieniu kluczy od pomieszczeń biurowych w wyznaczonym miejscu.

Klucze od biurek stanowiskowych i szaf biurowych będące w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.

Każdy pracownik we własnym zakresie zobligowany jest do przestrzegania:

a) **polityki „czystego ekranu”** - w przypadku chwilowego opuszczenia stanowiska pracy pracownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych,
b) **polityki „czystego biurka”** - w trakcie pracy pracownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy pracownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych,
c) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie),
d) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory),
e) pilnego strzeżenia akt, płyt CD/DVD, pamięci przenośnych i komputerów przenośnych,
f) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy,
g) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej,
h) zachowania tajemnicy danych, w tym także wobec najbliższych.

Komputery przenośne, na których są przetwarzane dane chronione poza siedzibą Urzędu Miasta i Gminy Ryn

Przetwarzanie danych na komputerach przenośnych poza siedzibą Urzędu, powinno być ograniczone do niezbędnego minimum i może się odbywać wyłącznie za zgodą Administratora. Każdy komputer przenośny musi być zabezpieczony indywidualnym identyfikatorem i hasłem. Pracownik korzystający z komputera przenośnego do przetwarzania danych, zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed ich zniszczeniem, utratą i uszkodzeniem.

W przypadku przetwarzania danych osobowych na komputerach przenośnych poza obszarem przetwarzania danych osobowych, użytkowników zobowiązuje się do:

a) przechowywania przedmiotowych danych na dysku szyfrowanym, zabezpieczonym hasłem co najmniej 8 - znakowym zawierającym: małe, wielkie litery, znaki specjalne lub cyfry,
b) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia,

c) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
d) zdecydowanego uniemożliwienia korzystania z komputera osobom niepowołanym (np. rodzinie, dzieciom, znajomym).

§ 9 Zarządzanie incydentami naruszenia bezpieczeństwa informacji

Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa danych osobowych informatycznej spoczywa na każdym pracowniku lub podmiocie przetwarzającym dane.

Klasyfikacja incydentów

Podział zdarzeń:

1) Zdarzenia losowe zewnętrzne (np.: klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) Zdarzenia losowe wewnętrzne (np. : niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) Zdarzenia zamierzone, świadome i celowe stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zdarzenia te możemy podzielić na:

- nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do danych z sieci wewnętrznej,
- nieuprawniony transfer danych,
- pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),
- bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

Przykłady zdarzeń, które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństw danych osobowych:

1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
2) Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).
3) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
4) Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
5) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.
6) Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.
7) Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
8) Nastąpiła niedopuszczalna manipulacja danymi w systemie.
9) Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.
10) Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
11) Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki”, itp.

12) Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe.
13) Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania PBI (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)
14) Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

Zgłaszanie incydentów

Pracownicy mają obowiązek notować wszystkie szczegóły związane z zauważonym przez siebie incydentem w raporcie oraz zgłaszać incydent **(najpóźniej do końca dnia roboczego, w którym zauważono incydent)** do swojego bezpośredniego Przełożonego.

Zgłaszający incydent powinien podjąć niezbędne działania, uwzględniając bezpieczeństwo i stopień ryzyka, zmierzające do zminimalizowania skutków zaistniałego incydentu w szczególności zabezpieczyć materiał dowodowy, np.: robiąc zdjęcie ekranu komputera co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. W przypadku podejrzenia istnienia wirusa komputerowego należy postępować zgodnie z Instrukcją w zakresie profilaktyki antywirusowej.

Postępowanie z incydentami:

Obsługa incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentu, identyfikacji i zabezpieczenia dowodów oraz poinformowania o zdarzaniu odpowiednich osób.

1) Przełożony, który przyjął zgłoszenie niezwłocznie przesyła drogą elektroniczną skan raportu do IOD;
2) Po analizie zdarzenia i okoliczności z nim związanych IOD celem rekomendacjami przedstawia sposób dalszego postępowania.
3) IOD po przygotowaniu rekomendacji przesyła drogą elektroniczną odpowiedni dokument do osoby odpowiedzialnej za kontakt z IOD.
4) Osoba upoważniona za kontakt z IOD przekazuje Administratorowi raport naruszenia ochrony danych oraz rekomendacje IOD. Następnie Administrator podejmuje decyzję co do sposobu rozliczenia incydentu.
5) Administrator wprowadza dane o incydencie do rejestru incydentów, do którego załącza się zabezpieczony materiał dowodowy.

Gromadzenie materiału dowodowego może polegać na:

- dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony;
- dla dokumentów na nośnikach komputerowych zaleca się: utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię).

W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem

naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w pkt. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.