SZKOŁA PODSTAWOWA Nr 2
im. Władysława Jagiełły
17-200 Hajnówka, ul. Wróblewskiego 2
REG. 000735121, NIP 543-20-47-459
tel. 85 682 28 66, fax: w. 118

Hajnówka, 31.07.2020 r.

Zarządzenie Dyrektora nr 12/2020

Szkoły Podstawowej nr 2 im. Władysława Jagiełły w Hajnówce
z dnia 31.07.2020 roku
w sprawie przyjęcia polityki ochrony danych osobowych

Na podstawie § Statutu Szkoły Podstawowej nr 2 im. Władysława Jagiełły w Hajnówce oraz art. 24 ust. 2 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 zarządza się, co następuje:

§1

Przyjmuje się politykę ochrony danych osobowych, która stanowi załącznik do niniejszego zarządzenia.

§2

Przyjmuje się wyliczone ryzyko znajdujące się w rejestrze czynności przetwarzania. Ryzyko zostało wyliczone na podstawie dokumentu „Analiza zagrożeń i ryzyka".

§3

Zarządzenie o przyjęciu polityki ochrony danych osobowych z dnia 31.08.2018 traci moc.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR SZKOŁY
mgr Adam Jerzy Chudek

SZKOŁA PODSTAWOWA Nr 2
im. Władysława Jagiełły
17-200 Hajnówka, ul. Wróblewskiego 2
REG. 000735121, NIP 543-20-47-459
tel. 85 682 28 66, fax: w. 118

Załącznik
do zarządzenia nr 12/2020
Dyrektora Szkoły Podstawowej nr 2 im. Władysława Jagiełły w Hajnówce
z dnia 31.07.2020 r.
w sprawie przyjęcia polityki ochrony danych osobowych

POLITYKA
OCHRONY DANYCH OSOBOWYCH
Szkoły Podstawowej nr 2 im. Władysława Jagiełły w Hajnówce

2060

Spis treści

PODSTAWY PRAWNE

§1

1. 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).
2. Ustawa z 10 maja 2018 r. o ochronie danych osobowych.

PODSTAWOWE POJĘCIA

§2

1. Administrator - w tym dokumencie jest rozumiany jako Szkoła Podstawowa nr 2 im. Władysława Jagiełły w Hajnówce.
2. RODO - w tym dokumencie rozumiane jako rozporządzenie 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).
3. Polityka - w tym dokumencie jest rozumiana jako „Polityka ochrony danych osobowych" obowiązująca u Administratora.
4. Inspektor Ochrony Danych (IOD) - osoba wyznaczona przez Administratora (Dyrektora) do nadzorowania przestrzegania zasad ochrony danych osobowych oraz przygotowania dokumentów wymaganych przez RODO. IOD powołany jest zarządzeniem Dyrektora Administratora.
5. Użytkownik - osoba upoważniona do przetwarzania danych osobowych. Użytkownikiem może być osoba zatrudniona, wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, porozumienia wolontarystycznego, odbywająca staż.

Cele i zasady funkcjonowania Polityki ochrony danych osobowych

§3

Realizując Politykę ochrony danych osobowych zapewnia się ich:

1. poufność - informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
2. integralność - dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
3. dostępność - istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
4. rozliczalność - możliwość jednoznacznego przypisania działań poszczególnym osobom,
5. autentyczność - zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
6. niezaprzeczalność - uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
7. niezawodność - zamierzone zachowania i skutki są spójne,
8. minimalizacji - zbierania jak najmniej danych osobowych i tylko takich jakie są wymagane do realizacji zadań Administratora.

§4

Polityka ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, to jest:

1. naruszeń danych osobowych rozumianych jako prywatne dobro powierzone,
2. naruszeń przepisów prawa oraz innych regulacji,
3. utraty lub obniżenia reputacji,
4. strat finansowych ponoszonych w wyniku nałożonych kar.

§5

Realizując politykę w zakresie ochrony danych osobowych Administrator dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1. przetwarzane zgodnie z prawem,
2. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
3. merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
4. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Zasady przetwarzania danych osobowych

§6

Administrator przestrzega następujących zasad przetwarzania danych osobowych:

1. Zasada zgodności z prawem, rzetelności i przejrzystości:

Komunikaty związane z przetwarzaniem danych osobowych są łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Informacje te są przekazywane w formie elektronicznej za pomocą stron internetowych. Ponadto Administrator w sposób bezpośredni powiadamia osoby, których dane dotyczą, wysyłając do nich bezpośrednio w formie tradycyjnej papierowej lub w formie elektronicznej klauzule informacyjne, w których podaje informacje przewidziane w Rozporządzeniu. Administrator podaje te informacje zarówno w przypadku zbierania danych od osoby, której dane dotyczą, jak i w przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą. Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawnił dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

2. Zasada ograniczenia celu przetwarzania danych:

Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach, wynikających z działań statutowych Administratora i nieprzetwarzane dalej niezgodnie z tymi celami. Osoby, których dane dotyczą, są informowane o celach przetwarzania, zgodnie z zasadami i w sposób określony w pkt. 1) powyżej. Administrator, w sytuacji gdy planuje przetwarzać dane w innym celu niż zostały zebrane, wysyła przed dalszym przetwarzaniem stosowną informację do osoby, której danej dotyczą i dostarcza jej wszystkich niezbędnych informacji w tym zakresie. Administrator może podjąć decyzję, że dane osobowe

będą przetwarzane do celów archiwalnych i statystycznych.

3. Zasada minimalizacji danych:

Dane osobowe przetwarzane są w sposób i w czasie niezbędnym do celów, w których są przetwarzane. Celami Administratora są jego prawnie uzasadnione cele wyrażające się w jego działalności statutowej. Administrator dokonuje okresowo selekcji danych i wybiera tylko taką ilość danych, jaka jest dla niego niezbędna do realizacji celów statutowych.

4. Zasada prawidłowości danych:

Administrator zapewnia prawidłowość i aktualność danych. Każda osoba, której dane dotyczą, może zgłosić Administratorowi prośbę o poprawienie, uaktualnienie, sprostowanie danych a także usunięcie danych, które są nieprawidłowe. Po zgłoszeniu pracownicy Administratora do tego upoważnieni dokonują poprawienia, aktualizacji, sprostowania lub usunięcia nieprawidłowych danych w zbiorze danych.

5. Zasada ograniczenia przechowania danych:

Dane osobowe są adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Celem Administratora jest realizacja prawnie uzasadnionego celu, tj. jego celów statutowych. Działalność Administratora jest nieograniczona w czasie. Dlatego też Administrator nie określa czasu przechowania danych. Wdraża natomiast procedurę okresowego przeglądu danych i wybiera tylko taką ilość danych, jaka jest dla niego niezbędna do realizacji celów statutowych.

6. Zasada integralności i poufności danych:

Dane osobowe są przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu. Służą temu rozwiązania organizacyjne i techniczne stosowane przez Administratora a opisane w niniejszej Polityce.

7. Zasada rozliczalności:

Administrator wykazuje przestrzeganie zasad przetwarzania danych osobowych poprzez:

a. informacje dla osób, których dane są przetwarzane na stronach internetowych,
b. informacje dla osób, których dane są przetwarzane przekazywane w sposób bezpośredni w formie elektronicznej lub papierowej w formie klauzul informacyjnych,
c. możliwość uzyskania przez każdą osobę w powszechnie używanym formacie jej danych osobowych,
d. możliwość uzyskania informacji dotyczących danych osobowych na specjalnie przeznaczonych do tego skrzynkach pocztowych,
e. dokumentowanie obsługi obowiązków informacyjnych, zawiadomień i żądań osób, których dane dotyczą,
f. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych),
g. rejestr czynności przetwarzania danych dokumentujący podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania,
h. upoważnienia do przetwarzania danych osobowych,
i. umowy z podmiotami, którym powierzono przetwarzanie danych,
j. ewidencja osób upoważnionych do przetwarzania danych osobowych,
k. inne rozwiązania organizacyjne i techniczne.

8. Prawo do przenoszenia danych:

Administrator zapewnia osobie, której dane dotyczą, otrzymanie w powszechnie używanym

formacie danych osobowych jej dotyczących. Osoba, której dane dotyczą, ma prawo przesłać te dane osobowe innemu Administratorowi. Żądanie przesłania danych osobowych może być zgłoszone drogą elektroniczną na skrzynkę podawczą Administratora podaną do powszechnej wiadomości na stronie internetowej lub drogą poczty tradycyjnej. Przesłanie danych odbywa się drogą elektroniczną na podany przez osobę, której dane dotyczą, adres e-mail lub drogą poczty tradycyjnej.

9. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach:

Administrator nie podejmuje decyzji w indywidualnych przypadkach, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu

Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów

§7

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety, smartfony, telefony, karty pamięci, dyski zewnętrzne itp.
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych.
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a. wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy,
   b. zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków, do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem).
9. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa.
10. Niedozwolone jest zabezpieczanie służbowych telefonów komórkowych przez użytkowników blokadami posługującymi się danymi biometrycznymi (np. odciskiem palca, twarzą). Możliwymi do zastosowania zabezpieczeniami są m.in. kod PIN oraz wzór blokady.
11. W przypadku korzystania ze sprzętu firmy Apple wykorzystującego między innymi system iOS oraz Mac OS należy:

a. wyłączyć automatyczną synchronizację plików z chmurą iCloud,
b. backup urządzenia należy robić po podłączeniu do komputera służbowego, który nie ma włączonej automatycznej synchronizacji plików z chmurą iCloud,

12. W przypadku braku możliwości wyłączenia automatycznej synchronizacji należy pracować w przeglądarkach internetowych oraz chmurach udostępnionych przez Administratora. Nie należy pobierać plików zawierających dane osobowe do pamięci sprzętu.

Zarządzanie uprawnieniami

§8

1. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji informatyków-administratorów.
3. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień Administratora.
4. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom praca na koncie innego użytkownika.

Polityka haseł

§9

1. Hasła powinny składać się z min. 8 znaków.
2. Hasła powinny zawierać małe litery, cyfry oraz znaki specjalne.
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami.
4. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
5. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
6. W przypadku ujawnienia hasła - należy natychmiast je zmienić.
7. Hasła muszą być zmieniane co 30 dni.
8. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
9. W przypadku przetwarzania danych we własnych systemach informatycznych (m.in. adresach mailowych w wykupionej domenie, stronach internetowych, aplikacjach) należy stosować uwierzytelnianie co najmniej dwustopniowe (np. podanie loginu oraz hasła + hasła wysłanego wiadomością na podany wcześniej numer telefonu / adres e-mail).

Zabezpieczenie dokumentacji papierowej z danymi osobowymi

§10

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu (zamykaniu) dokumentów w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np.: na terenach publicznych miejskich lub w lesie.
5. W przypadku braku stosownego uprawnienia przewidzianego w obowiązujących przepisach prawa, zabrania się tworzenia oraz przechowywania kopii dokumentów publicznych (np. dowodu osobistego, prawa jazdy) pod rygorem odpowiedzialności karnej przewidzianej w ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych.

Zasady wynoszenia nośników z danymi poza Szkołę

§11

1. Użytkownicy nie mogą wynosić na zewnątrz Szkoły wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora.
2. Dane osobowe wynoszone poza Szkołę muszą być zaszyfrowane (szyfrowane dyski, za hasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich.
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.

Zasady korzystania z Internetu

§12

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do Administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać

uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

Zasady korzystania z poczty elektronicznej

§13

1. Przesyłanie danych osobowych z użyciem e-maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 6 znaków: litery i cyfry, a hasło należy przesłać odrębnym środkiem komunikacji lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Nie należy otwierać załączników (plików) w e-mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu e- maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy.
6. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w e-mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy.
7. Należy zgłaszać Administratorowi przypadki podejrzanych e-maili.
8. Użytkownicy nie powinni rozsyłać „niezawodowych" e-maili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
9. Podczas wysyłania e-maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości - UDW". Zabronione jest rozsyłanie e-maili do wielu adresatów z użyciem opcji „Do wiadomości"!. Nie dotyczy to sytuacji, gdy wszyscy adresaci wiadomości ze sobą współpracują w ramach prowadzonych działań.
10. Użytkownicy powinni okresowo kasować niepotrzebne e-maile.
11. E-mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
12. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
13. Przy korzystaniu z e-maila, Użytkownicy mają obowiązek przestrzegać prawa własności

przemysłowej i prawa autorskiego.

14. Użytkownicy nie mają prawa korzystać z e-maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
15. Użytkownik bez zgody Administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Administratora, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
16. W przypadku konieczności wykonywania pracy na odległość („praca zdalna") pracownicy są obowiązani stosować się do zasad określonych w polityce ochrony danych osobowych.

Ochrona antywirusowa

§14

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.: Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora. Administrator obowiązany jest na bieżąco sprawdzać i aktualizować ochronę antywirusową na wszystkich urządzeniach służbowych.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§15

1. Konserwacja baz danych i oprogramowania przeprowadzana jest przez Administratora Systemu.
2. Konserwacja sprzętu komputerowego przeprowadzana jest przez Administratora Systemu lub firmę zewnętrzną.
3. W przypadku awarii sprzętu, na którym znajdują się dane osobowe w zależności od uszkodzenia następuje:
   a. naprawa na miejscu pod nadzorem Administratora Systemu,
   b. demontowanie dysku i zabezpieczenie u Administratora Systemu na czas naprawy,
   c. przegrywanie danych przez Administratora Systemu na inny nośniki usunięcia danych z przekazywanego do naprawy sprzętu.
4. W przypadku przekazania komputerów innemu użytkownikowi lub jednostce organizacyjnej, dane z dysków twardych są usuwane przez Administratora Systemu w sposób uniemożliwiający ich odtworzenie.
5. W przypadku złomowania sprzętu komputerowego, nośniki informacji (dyski twarde) są fizycznie niszczone przez Administratora Systemu.

Procedura tworzenia kopii zapasowych

§16

1. Kopie całościowe sporządzane są raz w miesiącu.
2. Kopie sporządzane są na płytach dyskach zewnętrznych lub płycie DVD/CD.
3. Każda nośnik jest opisany datą jej sporządzenia.
4. Kopie zapasowe przechowywane są tak długo jak wymagają tego przepisy prawa.
5. Dostęp do kopii mają osoby upoważnione przez Administratora.
6. Kopie przechowywane są miejscu zabezpieczonym na terenie siedziby Administratora.

Procedura napraw w serwisach zewnętrznych

§17

1. Komputery przeznaczone do naprawy należy wysyłać bez dysków, a urządzenia mobilne bez kart pamięci.
2. W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je wpierw trwale usunąć z użyciem specjalistycznego oprogramowania.
3. W przypadku braku możliwości usunięcia nośnika lub danych osobowych znajdujących się na nośniku, trzeba zawrzeć umowę powierzenia przetwarzania danych osobowych.
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta.

Regulamin użytkowania komputerów przenośnych

§18

1. Każdy użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Administratora, użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Administratora.
4. W przypadku kradzieży lub zgubienia komputera przenośnego, użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
   a. zaleca się przenoszenie go w specjalnym futerale. Dobrym sposobem na zmylenie potencjalnego złodzieja jest przenoszenie komputera przenośnego w zwykłej teczce-aktówce. Sugeruje to przenoszenie dokumentów, a ukrywa fakt transportu komputera przenośnego,
   b. zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru. W chwili obecnej złodzieje dysponują aparaturą umożliwiającą wykrywanie nawet ukrytych komputerów przenośnych,

c. podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego w sposób uniemożliwiający kradzież. Zabrania się przewożenia go np. na siedzeniach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach.

6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
7. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Procedura postępowania na wypadek wystąpienia naruszenia ochrony danych

§19

1. Procedura została opracowana w celu zapewnienia sprawnego oraz prawidłowego reagowania na wystąpienie naruszenia ochrony danych. Ma ona zastosowanie do wszelkich danych osobowych przetwarzanych przez Administratora zarówno w jego siedzibie, jak i poza nią.
2. Katalog przykładowych zagrożeń i naruszeń, jakie mogą wystąpić w związku z przetwarzaniem danych znajduje się w załączniku nr 7 do polityki ochrony danych osobowych.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Administratora bądź osób przez niego upoważnionych o przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych. Zawiadomienie ma nastąpić bez zbędnej zwłoki, ale w przeciągu 24 godzin od zaistnienia sytuacji.
4. Osoba, która stwierdzi fakt naruszenia ma obowiązek podjąć działania niezbędne do powstrzymania skutków naruszenia oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn i skutków naruszenia.
5. Administrator podejmuje działania w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Administrator przeprowadza analizę pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych (§20). W przypadku stwierdzenia:
   a. braku lub niskiego prawdopodobieństwa wystąpienia ryzyka Administrator zwolniony jest z obowiązku powiadamiania Prezesa UODO oraz osoby, której dane dotyczą o naruszeniu. Wnioski z przeprowadzonej analizy należy odnotować w wewnętrznym rejestrze naruszeń.
   b. wysokiego prawdopodobieństwa wystąpienia ryzyka Administrator ma obowiązek:
      – bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z zasadą przejrzystości. Należy uważać, aby nie wykorzystywać kanału kontaktowego, który w wyniku naruszenia przestał

być bezpieczny. Zasadą jest powiadamianie bezpośrednie (np. e-mail, SMS), natomiast gdy wymagałoby to niewspółmiernie dużego wysiłku Administrator powiadamia o naruszeniu komunikatem publicznym lub podobnym środkiem, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane o naruszeniu w równie skuteczny sposób,

- bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zawiadomić organ nadzorczy (Prezesa UODO). W przypadku nieposiadania przez Administratora w terminie wyznaczonym do udzielenia zgłoszenia wszystkich wymaganych informacji dotyczących naruszenia, zgłoszenie należy sukcesywnie uzupełniać podając przyczyny opóźnienia.

7. Naruszenia związane z atakami phishingowymi Administrator zgłasza również przez stronę www.incydent.cert.pl.

Analiza wystąpienia ryzyka naruszenia praw i wolności osób fizycznych

§20

1. Administrator „stwierdza" naruszenie, kiedy ma on wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych.
2. Konsekwencją stwierdzenia naruszenia jest konieczność przeprowadzenia analizy pod kątem ryzyka naruszenia praw lub wolności osób, których dane dotyczą. – od tego zależy czy naruszenie będzie podlegało zgłoszeniu do Prezesa UODO.
3. Administrator dokonuje analizy każdorazowo w odniesieniu do konkretnego naruszenia.
4. W ocenie ryzyka naruszenia praw i wolności osób fizycznych konieczne jest uwzględnienie:
   a. powagi zdarzenia tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą,
   b. prawdopodobieństwa wystąpienia tego zdarzenia będącego skutkiem naruszenia.
5. Stopień dotkliwości w przypadku zmaterializowania się zagrożenia należy oceniać z perspektywy osób, których dane są przetwarzane.
6. Dla poziomu potencjalnego ryzyka może mieć znaczenie fakt posiadania przez Administratora wiedzy, że dane osobowe znajdują się w rękach osób, których zamiary są nieznane lub które mogą mieć złe intencje.
7. Nie jest konieczne, aby ryzyko się zmaterializowało (by faktycznie doszło do naruszenia). Należy ocenić prawdopodobieństwo zaistnienia szkody w przypadku danego zdarzenia.
8. W przypadku jakichkolwiek wątpliwości Administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna.
9. Ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np.:
   a. dyskryminacja,
   b. kradzież tożsamości lub oszustwo dotyczące tożsamości,
   c. nadużycia finansowe,
   d. straty finansowe,
   e. nieuprawnione cofniecie pseudonimizacji,
   f. utrata poufności danych osobowych chronionych tajemnicą zawodową,

g. naruszenie dobrego imienia
h. lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej.

10. Jeżeli naruszenie dotyczy danych osobowych ujawniających:
    a. pochodzenie etniczne,
    b. poglądy polityczne,
    c. przekonania religijne lub światopoglądowe,
    d. przynależność do związków zawodowych,
    e. dane genetyczne,
    f. dane dotyczące zdrowia,
    g. dane dotyczące życia seksualnego,
    h. dane dotyczące wyroków skazujących lub naruszeń prawa,

    należy uznać, że w występuje duże prawdopodobieństwo takiej szkody. Niemniej jednak każde z takich zdarzeń należy rozpatrywać indywidualnie.
11. Kryteria oceny ryzyka dla osób fizycznych będącego wynikiem naruszenia:
    a. rodzaj naruszenia
    b. charakter, wrażliwość i ilość danych osobowych,
    c. łatwość identyfikacji osób fizycznych,
    d. waga konsekwencji dla osób fizycznych,
    e. cechy szczególne danej osoby fizycznej,
    f. cechy szczególne Administratora danych,
    g. liczba osób fizycznych, na które naruszenie wywiera wpływ.
12. Głównymi kryteriami branymi pod uwagę przy ocenie dotkliwości naruszenia danych osobowych są:
    a. kontekst przetwarzania danych (KPD) – określa typ naruszonych danych wraz z liczbą czynników związanych z ogólnym kontekstem przetwarzania,
    b. łatwość identyfikacji (ŁI) – określa jak łatwo można wywnioskować tożsamość osób z danych związanych z naruszeniem,
    c. okoliczności naruszenia (ON) – określają szczególne okoliczności naruszenia, które są związane z rodzajem naruszenia, w tym głównie z utratą bezpieczeństwa naruszonych danych, jak również wszelkie złośliwe zamiary.
13. Aby zdefiniować wynik dla kontekstu przetwarzania, Administrator danych powinien wykonać następujące kroki:
    a. określić rodzaje danych osobowych, których dotyczyło naruszenie,
    b. sklasyfikować dane w co najmniej jednej z czterech kategorii: dane podstawowe, dane szczególnej kategorii, dane finansowe, dane behawioralne (związane z nawykami). W ten sposób otrzymujemy podstawowy wynik KPD,
    c. punktacja – wynik podstawowy:
        - Dane podstawowe – 1 pkt.,
        - Dane behawioralne – 2 pkt.,
        - Dane finansowe – 3 pkt.,
        - Dane szczególnej kategorii – 4 pkt.
    d. Ocenić występowanie czynników bądź zakresów danych, które zwiększają lub zmniejszają wynik podstawowy.
14. Łatwość identyfikacji ocenia jak łatwo będzie dla strony, która ma dostęp do zestawu danych, jednoznacznie dopasować je do określonej osoby. Wyróżniamy cztery poziomy ŁI: znikome (0,25 pkt.), ograniczone (0,5 pkt.), znaczące (0,75 pkt.) i maksymalne (1,0 pkt.).
15. Przy określaniu okoliczności naruszenia należy brać pod uwagę utratę poufności, integralności i dostępności danych oraz złośliwe zamiary, które uzupełniają KPD I ŁI w następujący sposób:

a. Utrata poufności następuje, gdy strony uzyskują dostęp do informacji, do których nie są upoważnione. Stopień utraty poufności zależy od zakresu ujawnienia, tj. potencjalnej liczby i rodzaju stron, które mogą mieć bezprawny dostęp do informacji,
b. Utrata integralności występuje, gdy oryginalna informacja jest zmieniona i zastąpiona, a zmienione informacje mogą być szkodliwe dla jednostki,
c. Utrata dostępności następuje, gdy nie można uzyskać dostępu do oryginalnych danych. Sytuacja może być czasowa lub trwała,
d. Złośliwy zamiar to element, który określa, czy naruszenie było spowodowane błędem czy też działaniem zamierzonym. Obejmuje to przypadki kradzieży i włamania, jak również przekazywanie danych osobowych osobom trzecim w celu osiągnięcia zysku. Złośliwe intencje to czynnik, który zwiększa prawdopodobieństwo, że dane są wykorzystane w szkodliwy sposób dla jednostki. W zależności od rodzaju okoliczności naruszenia przyznajemy wartości 0, 0,25 lub 0,5.

16. Końcowy wynik oceny dotkliwości naruszenia oblicza się wzorem:
(DN): DN = KPD x ŁI + ON. Wyliczony wynik:
a. Niski: DN < 2
b. Średni: 2 ≤ DN < 3
c. Wysoki: 2 ≤ DN < 3
d. Bardzo wysoki: 4 ≤ DN
należy odnotować w rejestrze naruszeń.

Obowiązek zachowania poufności i ochrony danych osobowych

§21

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
   b. zachowania w tajemnicy danych osobowych do których mam lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora,
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora,
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią Polityki lub przeszkolone zobowiązane są podpisać oświadczenie o poufności.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
6. Na podstawie art. 30 ust. 4 RODO w związku z art. 4 pkt 21 RODO zabrania się udostępniania rejestru czynności przetwarzania danych osobowych innym podmiotom niż organowi

nadzorczemu, którym jest Prezes Urzędu Ochrony Danych Osobowych.

7. W przypadku gdy podmiot jest podmiotem przetwarzającym (np. w ramach projektu realizowanego ze środków europejskich) dozwolone jest częściowe udostępnienie rejestru kategorii czynności przetwarzania danych osobowych, ale wyłącznie w zakresie fragmentu dotyczącego kontrolowanej czynności.

Postępowanie dyscyplinarne

§22

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Administratora za naruszenie przepisów karnych zawartych w RODO i ustawie.

Polityka kluczy

§23

1. Polityka kluczy obejmuje pomieszczenia Administratora.
2. Upoważnienia do pobierania kluczy do pomieszczeń mają wyłącznie osoby wskazane przez Administratora.
3. Klucze do pomieszczeń wydawane i zdawane są za pobraniem z wyznaczonego pomieszczenia.
4. Klucze zapasowe przechowywane są w wyznaczonym pomieszczeniu. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą Administratora. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić.
5. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane oraz schowane w miejscu zabezpieczonym.
6. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność.
7. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
8. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
9. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń a w szczególności (wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi.
10. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

Udostępnianie i powierzanie danych osobowych

§24

1. Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie

nie naruszy praw i wolności osób, których one dotyczą.

2. Administrator odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.
3. Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której podmiot przyjmujący dane zobowiązuje się do przestrzegania obowiązujących przepisów RODO. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

Obowiązek informacyjny i wyrażenie zgody

§25

1. Każdy pracownik, który zbiera dane osobowe w imieniu Administratora, jest zobowiązany do przekazania zainteresowanemu obowiązku informacyjnego.
2. Dedykowany obowiązek informacyjny powinien być zamieszczony w każdym miejscu, gdzie są zbierane dane osobowe (np. na stronie internetowej, w formularzach zgłoszeniowych).
3. Zaleca się, by obowiązek informacyjny oraz zgoda na przetwarzanie danych osobowych była, o ile to możliwe, zawsze podpisana przez osobę, której dane dotyczą.
4. Jeżeli dane osobowe zostały pozyskane w inny sposób niż od osoby, której dane dotyczą, obowiązek informacyjny należy przedstawić tej osobie:
- w rozsądnym terminie po uzyskaniu danych osobowych – najpóźniej w ciągu miesiąca,
- jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji, z tą osobą, nie później niż w ciągu miesiąca,
- jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu, nie później niż w ciągu miesiąca.
5. Użyte w art. 81 ust. 2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych „zgromadzenie" jest pojęciem ocennym, które należy interpretować w oparciu o dany stan faktyczny. Rozpowszechnianie wizerunku danej osoby nie wymaga wyrażenia przez nią zgody, jeśli stanowi on jedynie element akcydentalny lub akcesoryjny przedstawionej całości, tzn. w razie usunięcia wizerunku nie zmieniłby się przedmiot i charakter przedstawienia.

Procedura usuwania i prostowania danych

§26

1. Pracownicy Administratora usuwając dane osobowe muszą skorzystać:
a. w przypadku danych przetwarzanych w formie papierowej (np. dokumenty, ale też wszelkie notatki, kalendarze itp.) wykorzystując niszczarkę,
b. w przypadku danych zapisanych na nośnikach danych, należy postąpić zgodnie z §15 ust. 4.
2. Jeżeli do Administratora wpłynie wniosek o usunięcie danych, to po sprawdzeniu czy dane osobowe nie są niezbędne:
a. do korzystania z prawa do wolności wypowiedzi i informacji,
b. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, 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;
d. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania,
e. do ustalenia, dochodzenia lub obrony roszczeń,
f. usuwa je zgodnie z zapisami ust. 1.

3. Jeżeli zachodzi jedna z przesłanek, opisanych w ust. 2, Administrator odmawia usunięcia danych.
4. Przez wniosek o usunięcie danych rozumie się również otrzymaną wiadomość e-mail, która nie zawiera treści.
5. Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
6. W przypadku opisanym w ust. 5 Administrator wprowadza niezbędne zmiany w danych, w posiadaniu, których jest.
7. Administrator zwraca uwagę na różnice w okresach retencji danych osobowych w stosunku do danych przetwarzanych za pomocą różnych środków (elektronicznych, papierowych) i usuwa je po upływie określonego okresu, zgodnie z przepisami prawa lub umowami powierzenia przetwarzania danych.
8. Administrator oraz osoba wyznaczona (np. osoba zajmująca się archiwizacją) ponoszą odpowiedzialność za przestrzeganie okresów retencji (archiwizacji) dokumentacji zawierającej dane osobowe i usuwanie jej w terminie zgodnym z obowiązującymi przepisami prawa lub w przypadku braku takich uregulowań, z ustalonymi okresami niezbędnymi do realizacji celów, dla których dane są przetwarzane.

Projektowanie prywatności

§27

ADO zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez ADO odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

Monitoring wizyjny

§28

1. Administrator musi na swoim terenie poinformować o monitoringu, poprzez zmieszczenie wyraźniej informacji na drzwiach, korytarzach, płotach itp. Tablice informujące o zainstalowanym monitoringu powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc, zaś wymiary tablic muszą być proporcjonalne do miejsca, gdzie zostały umieszczone. Stosowane mogą być dodatkowo piktogramy informujące o objęciu dozorem kamer. Nie jest wystarczające oznaczenie obszaru objętego monitoringiem jedynie

piktogramami

2. Należy zastosować obowiązek informacyjny, o którym mowa w §24, ale nie trzeba wywieszać go w każdym miejscu monitorowania. Obowiązek ten musi znajdować się miejscu widocznym.

3. Prawa osób objętych monitoringiem obejmują m.in.:

- prawo do informacji o istnieniu monitoringu w określonym miejscu, jego zasięgu, celu, nazwie podmiotu odpowiedzialnego za instalację, jego adresie i danych do kontaktu,
- prawo dostępu do nagrań w uzasadnionych przypadkach,
- prawo żądania usunięcia danych jej dotyczących,
- prawo do anonimizacji wizerunku na zarejestrowanych obrazach i/lub usunięcia dotyczących jej danych osobowych,
- prawo do przetwarzania danych przez ograniczony czas.

4. Okres przechowywania danych po dokonaniu nagrania nie może być dłuższy niż 30 dni.

5. Do ekranu, na którym odtwarzany jest monitoring mają dostęp tylko osoby upoważnione przez Administratora.

6. Rejestrator monitoringu jest obowiązkowo przechowywany w miejscu zamkniętym dla osób trzecich, a dostęp do niego mają tylko osoby upoważnione przez Administratora.

7. W przypadku wykorzystywania monitoringu do celów innych niż zapewnienie bezpieczeństwa, Administrator nie jest uprawniony do przetwarzania pochodzących z niego danych osobowych nawet na podstawie uzyskania wcześniejszych zgód od osób, które miały być nim objęte, gdyż nie jest możliwe, aby zebrać zgodę od wszystkich osób zarejestrowanych na nagraniach. Nie dotyczy to przypadku, kiedy wejście na monitorowany teren jest ograniczone w takim stopniu, że Administrator jest w stanie zebrać zgodę od każdej osoby, która pojawi się na nagraniu.

8. Stosowanie monitoringu dozwolone jest w celu: zapewnienia bezpieczeństwa, ochrony mienia, kontroli produkcji, zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

9. Monitoringu nie można stosować w celu: nadzoru nad jakością wykonywania pracy.

10. Niedozwolone jest instalowanie atrap kamer monitoringu.

11. Podejmując decyzję o wprowadzeniu monitoringu, Administrator musi przeprowadzić ocenę skutków dla ochrony danych. Jest ona wymagana, gdy operacja przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (np. w przypadku systematycznego monitorowania miejsc publicznych). Ocena zawiera:

a. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Administratora;
b. ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
d. środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§29

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, stosuje się wysoki poziom bezpieczeństwa. Administrator akceptuje poziom ryzyka oszacowany w rejestrze czynności przetwarzania, opracowany na podstawie „Analizy zagrożeń i ryzyka". IOD przeprowadza okresową (nie rzadziej niż raz na pół roku) analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawia Administratorowi propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

Załączniki

Załącznik nr 1 - Wzór upoważnienia do przetwarzania danych osobowych.
Załącznik nr 2 - Rejestr osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 3 - Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych.
Załącznik nr 4 - Rejestr naruszeń ochrony danych osobowych.
Załącznik nr 5 - Raport z naruszenia bezpieczeństwa danych osobowych.
Załącznik nr 6 - Rejestr zawartych umów powierzenia przetwarzania danych osobowych.
Załącznik nr 7 - Katalog przykładowych naruszeń.

Załącznik nr 1

....., dn .....

UPOWAŻNIENIE NR....
DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając w imieniu Szkoły Podstawowej nr 2 im. Władysława Jagiełły w Hajnówce na podstawie 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 oraz innych przepisów upoważniam:

.....
(imię, nazwisko, stanowisko)

do przetwarzania danych osobowych w następującym zakresie:

.....
(tu należy wskazać odpowiedni zakres przetwarzanych danych osobowych, określonych w analizie ryzyka w dziale „aktywa podstawowe")

Niniejsze upoważnienie jest wydane na czas oznaczony *[oznaczenie terminu]*

.....
(podpis osoby działającej w imieniu Administratora Danych Osobowych)

Załącznik nr 2

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data odebrania uprawnień	Uwagi

Załącznik nr 3

.....
(imię i nazwisko)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisana/y oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze zobowiązań wobec Szkoły Podstawowej nr 2 im. Władysława Jagiełły w Hajnówce zarówno w czasie trwania relacji (m.in. umowy, porozumienia), jak i po jej ustaniu.

Oświadczam, że zostałam/em poinformowany/a o obowiązujących zasadach dotyczących przetwarzania danych osobowych, określonych w Polityce ochrony danych osobowych i zobowiązuję się ich przestrzegać.

Zostałam/em zapoznana/y z przepisami o ochronie danych osobowych. Poinformowano mnie również o grożącej, stosownie do przepisów odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że złamanie zasad ochrony danych osobowych, obowiązujących w Szkoły Podstawowej nr 2 im. Władysława Jagiełły w Hajnówce może zostać uznane za ciężkie naruszenie podstawowych obowiązków i skutkować odpowiedzialnością dyscyplinarną.

.....
(podpis osoby upoważnionej)

Załącznik nr 5

....., dnia ..... r.

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Data: ..... r. Godzina: .....
2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....
   .....
   (imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)
3. Lokalizacja zdarzenia: .....
   .....
   (np. nr pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
   .....
   .....
   .....
5. Przyczyny wystąpienia zdarzenia:
   .....
   .....
6. Podjęte działania:
   .....
   .....

.....
(podpis zgłaszającego)

Załącznik nr 6

REJESTR ZAWARTYCH UMÓW POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Podmiot, z którym została zawarta umowa	Data zawarcia umowy	Data rozwiązania umowy	Uwagi

Załącznik nr 7

KATALOG PRZYKŁADOWYCH NARUSZEŃ

1. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych np. brak haseł, brak oprogramowania antywirusowego;
2. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników np. niestosowanie zasady czystego biurka, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek;
3. pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;
4. awarie serwera, komputerów, twardych dysków, oprogramowania;
5. pomyłki informatyków, użytkowników;
6. włamanie do systemu informatycznego lub pomieszczeń;
7. kradzież danych/sprzętu;
8. świadome zniszczenie dokumentów/danych;
9. działanie wirusów i innego szkodliwego oprogramowania np. poprzez szyfrowanie plików znajdujących się na urządzeniu;
10. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania;
11. niszczenie dokumentacji bez użycia niszczarki;
12. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
13. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
14. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
15. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Administratora;
16. zgubienie dokumentów przy ich przewożeniu;
17. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;
18. telefoniczne próby wyłudzenia danych osobowych;
19. kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive z danymi osobowymi;
20. e-maile zachęcające do ujawnienia identyfikatora i/lub hasła;
21. e-maile z linkiem/załącznikiem zawierającym wirusa;
22. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
23. hasła do systemów przyklejone są w pobliżu komputera;
24. utrata lub zagubienie danych np. chwilowe pozostawienie nośnika z danymi osobowymi w miejscu publicznym;
25. używanie poczty e-mail, „chmur" w serwisach, które nie są dostosowane do przepisów o ochronie danych osobowych;
26. przesyłanie danych osobowych (w szczególności danych wrażliwych) w niezaszyfrowanym e-mailu;
27. ujawnienie danych osobowych przez osobę, która została zwolniona z pracy lub została zobowiązana do zachowania poufności;
28. udzielenie odpowiedzi na pismo policji/urzędu/innej jednostki, w którym nie została przywołana podstawa prawna działań;
29. wykorzystywanie urządzeń służbowych do celów prywatnych;
30. przebywanie osób nieuprawnionych w pomieszczeniu przyjmowania interesantów;
31. przetwarzanie danych osobowych przez osobę, której nie zostało wydane upoważnienie do przetwarzania danych;
32. przechowywanie dokumentów zawierających dane osobowe po upływie okresu ich retencji;
33. utworzenie listy, na której zaznaczane są przyczyny nieobecności pracowników, w sposób umożliwiający innym pracownikom odczyt podanego powodu;
34. niewłaściwe niszczenie dokumentów umożliwiające odczyt „zniszczonych" danych osobowych np. poprzez używanie niszczarki paskowej zamiast ścinkowej;

35. ujawnienie dokumentacji wdrożeniowej RODO podmiotom nieuprawnionym;
36. posiadanie przez pracownika dostępu do zakresu danych osobowych niezgodnych z zajmowanym stanowiskiem, nie wydzielenie zakresów przetwarzania dla pracowników;
37. przekazywanie danych osobowych bez podpisanej umowy powierzenia lub bez podstawy prawnej;
38. udostępnienie zdjęć na stronie internetowej/portalach społecznościowych bez wcześniejszego uzyskania zgody;
39. wysłanie e-maila bez ukrycia adresów e-mail odbiorców (DW zamiast UDW).

Naruszenie należy niezwłocznie zgłosić przełożonemu, który wspólnie z Administratorem oraz Inspektorem Ochrony Danych (w przypadku jego wyznaczenia), podejmuje odpowiednie kroki w celu usunięcia bądź zminimalizowania skutków naruszenia.

DYREKTOR SZKOŁY
mgr Adam Jerzy Chudek