REGULAMIN Ochrony Danych Osobowych Fundacji Wspierania Kultury „ARS” – dalej Fundacji

Spis treści:

Rozdział 1: Postanowienia ogólne

- Regulamin stanowi wykaz podstawowych obowiązków z zakresu przetwarzania zasad ochrony danych osobowych w Fundacji Wspierania Kultury „ARS” zgodnie z Rozporządzeniem PE i RE 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.
- Regulamin obowiązuje wszystkich osób związanych z działalnością statutową Fundacji, podmioty przetwarzające dane osobowe na podstawie zawartych umów między przetwarzającymi a powierzającymi użytkowników systemów informatycznych z dostępem do danych osobowych upoważnionych przez Administratora na piśmie.
- Każdy z wymienionych podmiotów zobowiązany jest do zapoznania się z dokumentem i bezwzględnego przestrzegania zawartych w nim zasad.
- Administratorem danych osobowych w Fundacji jest Prezes zarządu.

Rozdział 2: Polityka korzystania z internetu

- Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach statutowych Fundacji.
- Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego żródła.Pliki takie

powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.

- Użytkownik ponosi odpowiedzialność za szkody w infrastrukturze IT spowodowane przez oprogramowanie instalowane z internetu.
- Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym pzrze prawo ze względu na zainstalowane na nich szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem.
- Zabrania się w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
- W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki(kłódka) oraz adresu www rozpoczynającego się frazą.W tej sytuacji należy”kliknąć” w ikonę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
- Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na (np.na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej)lub podania naszych loginów i haseł, PINów, numerów kart płatniczych przez internet.

Rozdział 3; Polityka korzystania z poczty elektronicznej

- Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do korzystania z poczty elektronicznej Fundacji tylko w celach jej działalności statutowej.
- W przypadku przesyłania danych osobowych poza Fundację należy wykorzystywać mechanizmy kryptograficzne(hasłowanie wysyłanych dokumentów lub zzipowanych plików, podpis elektroniczny).
- W przypadku zabezpieczenia plików hasłem, obowiązuje 8 znaków:duże i małe litery lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np.telefonicznie lub SMSem.
- Każdy użytkownik przed wysłaniem poczty zobowiązany jest sprawdzić poprawność adresu odbiorcy dokumentu.
- Zaleca się aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
- W celu ochrony przed zainfekowaniem komputera użytkownika i komputerów pracujących w sieci(kryptowirusy) zabrania się otwierania załączników(plików) w mailach nawet od prawdopodobnie znanych użytkowników nadawców bez weryfikacji nadawcy.

- Zabrania się, bez weryfikacji wiarygodności nadawcy"klikać" na hiperlinki w mailach. Nieprzestrzeganie tej zasady może doprowadzić do zainfekowania komputera użytkownika i innych pracujących w sieci.
- Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać administratorowi.
- Przy wysyłaniu maili do wielu adresatów jednocześnie, należy użyć metody"ukryte do wiadomości -UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji"Do wiadomości".
- Zabrania się rozsyłania maili z tzw."łańcuszkami szczęcia". Adres mailowy - służbowy Fundacji służy wyłącznie do korespondencji służbowej.
- Nakazuje się okresowe czyszczenie poczty z nieaktualnych emaili i opróżnianie kosza.
- Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe osób związanych z działalnością statutową Fundacji lub innych osób.
- Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno to być ograniczone do niezbędnego minimum.
- Korzystanie z poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków.
- Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechnienia treści o charakterze obraźliwym, niemoralnym lub nieetycznym i naruszającym cudzą godność i prywatność.
- Użytkownik bez zgody Prezesa Fundacji nie ma prawa wysyłać wiadomości zawierających dane osobowe pracodawców/zleceniodawców, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
- Wszelkie przesyłanie dokumentów, opracowania, jak i innych treści przesyłane przez użytkownika podlegają ochronie prawa autorskiego i prawa własności, które użytkownik winien jest przestrzegać.

Rozdział 4; Polityka użytkowania komputerów przenośnych

- Każdy użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
- W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę pracodawcy – użytkownik zobowiązany jest do ich przetwarzania na dysku szyfrowanym, zabezpieczonym co najmniej 8-znakowym hasłem(duże, małe litery, znaki specjalne lub cyfry).

- Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnice Fundacji w tym potencjonalnego pracodawcy.
- W przypadku kradzieży lub zgubienia komputera przenośnego-użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych, tj.Administratora Danych lub IOD, zaznaczając jednocześnie, jakiego rodzaju dane były na urządzeniu przechowywane.
- Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
- zaleca się przenoszenie go w specjalnym futerale,
- zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru,
- podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy.
- 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.
- Jeżeli jest możliwość pozostawienia komputera przenośnego w siedzibie Fundacji to powinno się taką możliwość rozważyć.
- Użytkownik komputera przenośnego zobowiązany jest do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach typu:pendrive lub dyski zewnętrzne.Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu z uwzględnieniem ochrony przed dostępem osób niepowołanych.
- Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Rozdział 5; Polityka wynoszenia nośników z danymi osobowymi poza siedzibę Fundacji

- Użytkownicy nie mogą wynosić poza Fundację bez zgody Administratora danych żadnych wymiennych elektronicznych nośników informacji typu: wymienne twarde dyski, pendrive lub inne nośniki typu – zewnętrzny dysk.
- W sytuacjach koniecznych, za zgodą Administratora danych, wynoszone nośniki wymienne muszą być zaszyfrowane, a pliki opatrzone hasłem.
- Zabrania się wynoszenia poza Fundację dokumentacji papierowe zawierającej dane osobowe. W przypadku wynoszenia tej dokumentacji poza Fundację należy ją przenosić w zamykanych teczkach lub w innej bezpiecznej formie.

- W przypadku przesyłania dokumentacji j/w należy korzystać z zaufanych firm kurierskich, za pokwitowaniem i w opakowaniach gwarantujących niedostępność osób trzecich.

Rozdział 6;Polityka zabezpieczania dokumentacji papierowej z danymi osobowymi

- Upoważnione osoby przez Fundację są zobowiązane do stosowania tzw."Polityki czystego biurka".Polega ona na zabezpieczaniu(zamykaniu) dokumentów np.w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy,podczas nieobecności i w trakcie pracy.
- Z upoważnienie Administratora danych można niszczyć dokumenty i wydruki w niszczarkach lub utylizować w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
- Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabiezpieczonymi pomieszczeniami w tym na kserokopiarkach, drukarkach, w pomieszczeniach ogólnodostępnych.
- Zabrania się wyrzucania zniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz np. na terenach publicznych miejski, lesie.

Rozdział 7;Polityka tworzenia kopii zapasowych

- Zbiory danych osobowych w systemach informatycznych są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
- urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej, sporządzania kopii zapasowych(kopie pełne)
- pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku.Kopie systemu kadrowo-płacowego całościowe sporządzane są raz w miesiącu, a kopie przyrostowe raz dziennie.
- W szczególnych sytuacjach, np.przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię systemu.
- Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem przydatności do odtworzenia w przypadku awarii systemu.
- Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.
- Kopie całościowe przechowywane są przez 5 lat a kopie przyrostowe przez 1 miesiąc.

Rozdział 8;Polityka niszczenia danych osobowych na nośnikach elektronicznych

- W odniesieniu do nośników przenośnych(pendrive)oraz nośników danych zainstalowanych na komponentach elektronicznych – złomowanych stosowane są mechanizmy bezpiecznego kasowania informacji:
- za pomocą specjalistycznego oprogramowania
- przy użyciu demagnetyzacji
- poprzez fizyczne niszczenie(pocięcie, spalenie)nośników.
- Wyznaczony Administrator dokonuje kontroli prawidłowości usunięcia informacji.
- Nośniki usuwalne, które nie mogą być ponownie wykorzystane, są niszczone.
- Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik.
- Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada Administrator danych.
- Niszczenie nośnika zastaje odnotowane w protokole zniszczenia.

Rozdział 9; Polityka niszczenia danych na nośnikach papierowych

- Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz niszczarkach o podwyższonym standardzie. Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji.

Rozdział 10; Polityka napraw sprzętu IT w serwisach zewnętrznych

- Komputery przeznaczone do naprawy należy wysyłać bez dysków a urządzenia mobilne bez kart pamięci.
- W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je wpierw trwale usunąć z użyciem specjalistycznego oprogramowania.
- W przypadku naprawy sprzętu z danymi osobowymi na nośniku – rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującej bezpieczną naprawę- należy zwrócić uwagę przy zakupach sprzętu.
- 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 podawania hasła.
- Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta(umowy gwarancyjne on-site).

Rozdział 11; Postępowanie dyscyplinarne

- Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków naruszenia zasad współpracy.
- Postępowanie sprzeczne z powyższymi zasadami może być uznane przez zarząd Fundacji w osobie Prezesa – za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016r.

Racibórz, dn. 12.10.2024.r.