Załącznik do uchwały nr 349 z dnia 24 maja 2018 r.
Zarządu Głównego Polskiego Czerwonego Krzyża

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH w Polskim Czerwonym Krzyżu

Pieczęć organizacji:	Podpis w imieniu Administratora Danych Osobowych:	Data:
POLSKI CZERWONY KRZYŻ 00-561 Warszawa, ul. Mokotowska 14 Regon 007023731, NIP 526-025-04-81	Dorota Małecka DYREKTOR GENERALNY Polskiego Czerwonego Krzyża Marzena Jurczak p.o. Głównego Księgowego Polskiego Czerwonego Krzyża	24 maja 2018 r.

Spis treści

Wstęp

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia 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) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się w Polskim Czerwonym Krzyżu następujący zestaw procedur.

Rozdział 1. Postanowienia ogólne

§ 1.

1. Ilekroć w dokumencie jest mowa o:
   a) **rozporządzeniu** – rozumie się przez to 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) – dalej RODO;
   b) **danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
   c) **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
   d) **przetwarzaniu danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
   e) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   f) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

g) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
h) **administratorze danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
i) **zgodzie osoby, której dane dotyczą** – oznacza to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
j) **odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
k) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
l) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
m) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
n) **profilowaniu** – oznacza to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
o) **pseudonimizacji** – oznacza to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
p) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
q) **naruszeniu ochrony danych osobowych** – oznacza to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do

danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Rozdział 2. Zasady ochrony danych osobowych

§ 2.

1. Dane osobowe muszą być:
a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą **(„zgodność z prawem, rzetelność i przejrzystość")**,
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami **(„ograniczenie celu")**,
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane **(„minimalizacja danych")**,
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane **(„prawidłowość")**,
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą **(„ograniczenie przechowywania")**,
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych **(„integralność i poufność")**,
2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie **(„rozliczalność")**.

Rozdział 3. Administrator danych

§ 3.

1. Administratorem danych osobowych jest Polski Czerwony Krzyż.
2. Zgodnie ze Statutem PCK, przyjętym Rozporządzeniem Rady Ministrów z dnia 20 września 2011 r. w sprawie zatwierdzenia statutu Polskiego Czerwonego Krzyża (Dz.U. 2011 nr 217 poz. 1284 z zm.) w imieniu administratora danych osobowych występuje Zarząd Główny PCK.
3. Administrator danych w szczególności uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Administrator Danych Osobowych - Polski Czerwony Krzyż wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie

odbywało się zgodnie z RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

4. W Polskim Czerwonym Krzyżu prowadzony jest rejestr czynności przetwarzania zgodnie z Załącznikiem nr 1.
5. Dla właściwej realizacji ochrony danych osobowych wyznacza się w Polskim Czerwonym Krzyżu Inspektora Ochrony Danych (IOD) zgodnie z Załącznikiem nr 2.
6. Każdorazowy Zarząd Oddziału Okręgowego PCK jest odpowiedzialny za umocowanie pełnomocnika ds. ochrony danych tj. osoby odpowiedzialnej za realizację zadań wynikających z niniejszej Polityki w każdym podległym mu Oddziale Okręgowym PCK zgodnie z Załącznikiem nr 3.
7. Do obowiązków PODO należy:
   a) zapewnienie przeszkolenia osób przetwarzających dane osobowe pod bezpośrednim nadzorem lub na zlecenie PCK,
   b) zapewnienie nadania upoważnień do przetwarzania danych osobowych przez osoby umocowane do ich nadawania w imieniu administratora danych osobom przeszkolonym oraz odebranie od tych oświadczeń o przestrzeganiu wewnętrznej dokumentacji ochrony danych osobowych i zachowaniu danych osobowych w poufności,
   c) przeprowadzanie oceny skutków przetwarzania zgodnie z Rozdziałem 6 Polityki bezpieczeństwa przetwarzania danych osobowych w PCK,
   d) przeprowadzanie analizy ryzyka wobec zasobów biorących udział w procesach przetwarzania danych osobowych zgodnie z Rozdziałem 7 Polityki ochrony danych osobowych w PCK,
   e) zapewnienie przestrzegania przez osoby upoważnione procedury domyślnej ochron danych osobowych i ochrony danych osobowych na etapie projektowania zgodnie z Rozdziałem 9 Polityki bezpieczeństwa przetwarzania danych osobowych w PCK,
   f) zapewnienie zgłaszania naruszeń ochrony danych osobowych Inspektorowi Ochrony Danych oraz wdrożenie zasad opisanych Rozdziale 2 Polityki ochrony danych osobowych w PCK,
   g) zapewnienie zawarcia umów powierzenia przetwarzania danych osobowych z podmiotami przetwarzającymi zgodnie z Rozdziałem 8 Polityki ochrony danych osobowych w PCK.
8. Pełnomocnik ds. ochrony danych wykonując czynności związane z realizacją niniejszej Polityki współpracuje z Inspektorem Ochrony Danych reagując na każde naruszenie w obszarze ochrony danych osobowych w Oddziale Okręgowym PCK i niezwłocznie pisemnie informuje o tym fakcie Zarząd Okręgowy PCK , Inspektora Ochrony Danych i Dyrektora Okręgowego PCK.

Rozdział 4. Inspektor ochrony danych

§ 4.

1. Inspektor ochrony danych ma następujące zadania:
   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
d) współpraca z organem nadzorczym,
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami z organem nadzorczym oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
3. Inspektor Ochrony Danych podlega bezpośrednio Zarządowi Głównemu PCK .

Rozdział 5. Środki techniczne i organizacyjne

§ 5.

W celu ochrony danych spełniono wymogi, o których mowa w rozporządzeniu, w szczególności:

a) przeprowadzono ocenę skutków dla ochrony danych w poszczególnych procesach przetwarzania danych osobowych zgodnie z załącznikiem nr 4,
b) przeprowadzono analizę ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach zgodnie z załącznikiem nr 5a i 5b,
c) do przetwarzania danych zostały dopuszczone wyłącznie osoby upoważnione przez administratora danych zgodnie z załącznikiem nr 6,
d) zawarto umowy powierzenia przetwarzania danych zgodnie z załącznikiem nr 7,
e) została opracowana i wdrożona niniejsza polityka bezpieczeństwa i wydano na jej podstawie Regulamin ochrony danych osobowych zgodnie z Załącznikiem nr 12.

§ 6.

W celu ochrony danych osobowych stosuje się w Polskim Czerwonym Krzyżu następujące środki ochrony fizycznej danych osobowych:

a) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nieprzeciwpożarowymi);
b) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min;
c) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie – drzwi klasy C;
d) zbiory danych osobowych przechowywane są w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej;
e) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, objęty jest systemem kontroli dostępu;

f) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie;
g) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej metalowej szafie;
h) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętym sejfie lub kasie pancernej;
i) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy;
j) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 7.

W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
b) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
c) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych;
d) zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł;
e) zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych;
f) zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji;
g) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej;
h) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
i) użyto system Firewall do ochrony dostępu do sieci komputerowej;

§ 8.

W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:

a) wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
b) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
c) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
d) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;
e) zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych;

§ 9.

1. W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:
   a) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
   b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;
   c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
   d) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
   e) kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Rozdział 6. Procedura DPIA (Data Protection Impact Assessment)

§ 10.

Ocenę skutków przetwarzania (DPIA) przeprowadza każdorazowy pełnomocnik ds. ochrony danych osobowych wskazany przez administratora danych zgodnie z §3 pkt 6 niniejszej Polityki z wykorzystaniem załącznika nr 4.

§ 11.

DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana dostawcy usług, zmiana sposobu przetwarzania danych, wymiana zasobów biorących udział w procesie.

§ 12.

DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które w wyniku poprzednio przeprowadzonego DPIA wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą lub procesów, które znajdują się na liście procesów wymagających przeprowadzania DPIA publikowanej przez organ nadzorczy.

Rozdział 7. Procedura analizy ryzyka i plan postępowania z ryzykiem

§ 13.

Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowy pełnomocnik ds. ochrony danych osobowych wskazany przez administratora danych zgodnie z §3 pkt 6 niniejszej Polityki z wykorzystaniem załącznika nr 5a i 5b.

§ 14.

Analiza ryzyka, o której mowa w § 11 jest przeprowadzana nie rzadziej niż raz w roku kalendarzowym i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.

§ 15.

Na podstawie wyników przeprowadzonej analizy ryzyka, każdorazowy pełnomocnik ds. ochrony danych osobowych wskazany przez administratora danych samodzielnie wdrażają sposoby postępowania z ryzykiem. Jeżeli plan postepowania z ryzykiem wymaga dodatkowych zasobów ww. pełnomocnik wnioskuje o ich zapewnienie do administratora danych.

§ 16.

Każdorazowo w razie powstania wątpliwości co do wyboru metody postepowania z ryzykiem administrator danych, po zasięgnięciu opinii IOD wybiera sposób postępowania z ryzykiem i określa, które metody postępowania z ryzykiem i w jakiej kolejności będą wdrażane.

§ 17.

Pełnomocnik, o którym mowa w §3 pkt 6 niniejszej Polityki nie może zlekceważyć ryzyk, których wartość przekracza 6 punktów zgodnie z załącznikiem nr 5b lub ryzyka w stosunku do zasobu, biorącego udział w procesie wysokiego ryzyka zgodnie z wynikiem DPIA zgodnie z załącznikiem nr 4.

Rozdział 8. Procedura współpracy z podmiotami zewnętrznymi

§ 18.

Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone oceną tego podmiotu zgodnie z Załącznikiem nr 7 oraz w razie pozytywnego wyniku oceny zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie z załącznikiem nr 8.

§ 19.

Nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z RODO wszystkich podmiotów przetwarzających, z których usług korzysta zgodnie z Załącznikiem nr 7.

Rozdział 9. Procedura domyślnej ochrony danych i ochrony danych na etapie projektowania

§ 20.

Administrator danych w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza DPIA w stosunku do tego procesu zgodnie z Rozdziałem 6 niniejszej Polityki.

§ 21.

W każdym przypadku tworzenia nowego produktu lub usług administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania poprzez prowadzenie konsultacji z IOD.

Rozdział 10. Procedura zarządzania incydentami

§ 22.

1. W każdym przypadku stwierdzonego naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

2. Każde zdarzenie prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych podlega zgłoszeniu do IOD za pośrednictwem adresu: iod@pck.org.pl w terminie 24h od jego wystąpienia.
3. IOD dokonuje oceny czy stwierdzone naruszenie ochrony danych osobowych skutkowało naruszeniem praw lub wolności osób fizycznych i przekazuje rekomendacje w zakresie dalszego postępowania do administratora danych w terminie 24h.
4. W przypadku nieobecności w pracy IOD każdy przypadek naruszenia danych osobowych PCK zgłaszany jest bez jakiejkolwiek zwłoki bezpośrednio do Dyrektora Generalnego PCK.

§ 23.

Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia. W przypadku nieobecności IOD organ nadzorczy informowany jest bezpośrednio przez Dyrektora Generalnego PCK.

§ 24.

Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.

§ 25.

Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych zgodnie z Załącznikiem nr 9.

Rozdział 11. Procedura realizacji praw osób

§ 26.

W każdym procesie pobierania danych osobowych od osób, których dane dotyczą lub w procesie pobierania danych osobowych z innych źródeł niż osoba, której dane dotyczą spełnia się wobec nich obowiązek informacyjny zgodnie z Załącznikiem nr 10. Za spełnienie obowiązku informacyjnego odpowiedzialny jest pełnomocnik ds. ochrony danych osobowych wskazany przez administratora danych zgodnie z §3 pkt 6 niniejszej Polityki.

§ 27.

1. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w RODO administrator danych rozpatruje indywidualnie.
2. Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:
   a) prawo dostępu do danych,
   b) prawo do sprostowania danych,
   c) prawo do usunięcia danych,
   d) prawo do ograniczenia przetwarzania danych,

e) prawo do przenoszenia danych,
f) prawo do sprzeciwu wobec przetwarzania danych,
g) prawo do niepodlegania decyzjom oparty wyłącznie na profilowaniu.

3. Każde ww. żądanie osoby, której dane dotyczą zostaje wysłane do IOD na adres iod@pck.org.pl
4. W celu realizacji ww. praw IOD przeprowadza analizę zasadności skorzystania z prawa przez osobę, której dane dotyczą i niezwłocznie udziela jej odpowiedzi na podstawie wyników Załącznika nr 11.

§ 28.

W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych pełnomocnik ds. ochrony danych osobowych wskazany przez administratora danych zgodnie z §3 pkt 6 niniejszej Polityki niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku zgodnie z rekomendacją IOD.

§ 29.

Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów RODO, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z RODO.

Rozdział 12. Procedura odbierania zgód

§ 30.

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie ww. warunku nie jest wiążąca.
3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę.
4. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.
5. W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody zgodnie z Załącznikiem nr 10 przy dochowaniu obowiązków określonych w Rozdziale 11 niniejszej Polityki.

Rozdział 13. Postanowienia końcowe

§ 31.

Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dóbr osób, których dane te dotyczą.

§ 32.

Dokument niniejszy obowiązuje od przyjęcia uchwały Zarządu Głównego PCK nr 349 z dnia 24 maja 2018 r. w sprawie przyjęcia dokumentacji ochrony danych osobowych.

Załączniki:

załącznik nr 1 - rejestr czynności przetwarzania,
załącznik nr 2 - powołanie IOD,
załącznik nr 3 - powołanie pełnomocnika ds. ochrony danych osobowych,
załącznik nr 4 - ocena skutków przetwarzania,
załącznik nr 5a - inwentaryzacja zasobów,
załącznik nr 5b - analiza ryzyka wobec zasobów,
załącznik nr 6 - upoważnienie do przetwarzania danych osobowych,
załącznik nr 7 - lista kontrolna procesora,
załącznik nr 8 - umowa powierzenia przetwarzania danych osobowych,
załącznik nr 9 - rejestr incydentów,
załącznik nr 10 - klauzule zgody i treści obowiązku informacyjnego,
załącznik nr 11 - arkusz realizacji praw osób,
załącznik nr 12 – regulamin ochrony danych osobowych.