



**POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH  
DLA DIGICOS S.A.**

## Spis treści

§ 1. CELE POLITYKI BEZPIECZEŃSTWA.....	3
§ 2. DEFINICJE.....	3
§ 3. ZASIĘG ORAZ ZAKRES OBOWIĄZYWANIA POLITYKI .....	5
§ 4. ZASADY OGÓLNE PRZETWARZANIA DANYCH OSOBOWYCH.....	6
§ 5. BEZPIECZEŃSTWO DANYCH OSOBOWYCH.....	8
§ 6. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH.....	10
§ 7. ORGANIZACJA PRACY PRZY PRZETWARZANIU DANYCH .....	12
§ 8. KONTAKT Z OSOBAMI, KTÓRYCH DANE DOTYCZĄ.....	13
§ 9. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ .....	15
§ 10. ZADANIA OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ DANYCH .....	16
§ 11. ODBIORCY DANYCH.....	18
§ 12. POSTĘPOWANIE Z INCYDENTAMI.....	19
§ 13. ODPOWIEDZIALNOŚĆ.....	20
ZAŁĄCZNIK NR 1. Rejestr Czynności Przetwarzania .....	Błąd! Nie zdefiniowano zakładki.
ZAŁĄCZNIK NR 2. Wytyczne dotyczące oceny skutków dla ochrony danych.....	Błąd! Nie zdefiniowano zakładki.
ZAŁĄCZNIK NR 3. Wzór upoważnienia .....	2Błąd! Nie zdefiniowano zakładki.
ZAŁĄCZNIK NR 4. Rejestr upoważnionych .....	24

## § 1. CELE POLITYKI BEZPIECZEŃSTWA

1. Polityka Bezpieczeństwa Danych Osobowych (dalej: Polityka) dotyczy danych osobowych przetwarzanych w DIGICOS Spółka akcyjna (dalej: DIGICOS).
2. Polityka opisuje stosowane przez DIGICOS środki organizacyjne i techniczne, nakierowane na zapewnienie zgodności z prawem, rzetelności i przejrzystości, celowości procesów przetwarzania danych osobowych. Polityka opisuje także sposób realizacji zasady ograniczenia celu przetwarzania danych osobowych, minimalizacji zakresu zbieranych danych, utrzymania ich prawidłowości, ograniczenia czasowego przetwarzania oraz zapewnienia ich poufności i integralności. Realizacja powyższych zasad jest kluczowa dla prawidłowego zarządzania danymi osobowymi w DIGICOS.
3. Polityka, wraz z Instrukcją Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych, Instrukcją Bezpieczeństwa Sieci Komputerowej, Zasadami Użytkowania Komputerów Osobistych, Sprzętu Informatycznego oraz Sieci Teleinformatycznej i Instrukcją Tworzenia i Przechowywania Kopii Zapasowych ma stanowić zespół wytycznych, które osoby mające dostęp do danych osobowych przetwarzanych w DIGICOS winny przestrzegać. Dotyczy to w szczególności pracowników DIGICOS, ale także innych osób, które otrzymują dostęp do danych osobowych, których dana spółka jest administratorem.
4. Postanowienia Polityki pozostają w zgodzie z postanowieniami zawartymi w:
  - 1) Konstytucji Rzeczypospolitej Polski z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483), ze szczególnym uwzględnieniem postanowień artykułów 47 i 51,
  - 2) Rozporządzeniu 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**).
  - 3) Ustawie z dnia 10 maja 2018 r. roku o ochronie danych osobowych

Przestrzeganie postanowień Polityki i pozostałych dokumentów wymienionych w ust. 3, nie zwalnia osób je stosujących z działania w zgodzie z wyżej wskazanymi przepisami prawa, w zakresie, w jakim rozszerzają one postanowienia tu zawarte.

## § 2. DEFINICJE

Na potrzeby niniejszej Polityki, a także Załączników, wskazanym poniżej terminom nadaje się następujące znaczenie:

- 1) „DIGICOS”, „Spółka”, „ADO” – określenie podmiotu z § 1 ust. 1

- 2) **„Administrator Sieci Informatycznej”, „ASI”** – osoba odpowiedzialna w DIGICOS za zarządzanie systemem informatycznym, w którym przetwarzane są dane osobowe i odpowiadająca za jego sprawne działanie;
- 3) **„dane osobowe”** – wszelkie 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
- 4) **„Inspektor Ochrony Danych”, „IOD”** - osoba fizyczna, która może zostać wyznaczona w DIGICOS, która sprawuje nadzór nad przestrzeganiem zasad ochrony wynikających z RODO, innych przepisów Unii Europejskiej lub przepisów krajowych o ochronie danych i zobowiązana jest prowadzić dokumentację wynikającą z tychże przepisów;
- 5) **„profilowanie”** - dowolna forma 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;
- 6) **„pseudonimizacja”** - 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;
- 7) **„przetwarzanie danych osobowych”, „przetwarzanie”** – każda operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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;
- 8) **„RODO”** – 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;
- 9) **„Ustawa”** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
- 10) **„zbiór danych osobowych”, „zbiór”** – każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie; zbiór danych może być prowadzony zarówno w formie elektronicznej jak i papierowej.

### § 3. ZASIĘG ORAZ ZAKRES OBOWIĄZYWANIA POLITYKI

1. Celem niniejszej Polityki jest określenie zasad przetwarzania danych osobowych oraz ich bezpieczeństwa, jako zestawu praw, reguł, procedur i praktycznych doświadczeń regulujących sposób ich przetwarzania, zarządzania, ochrony i dystrybucji wewnątrz DIGICOS, jak i w kontaktach z otoczeniem.
2. Polityka wraz z Instrukcją Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych, Instrukcją Bezpieczeństwa Sieci Komputerowej, Zasadami Użytkowania Komputerów Osobistych, Sprzętu Informatycznego oraz Sieci Teleinformatycznej i Instrukcją Tworzenia i Przechowywania Kopii Zapasowych opisują zabezpieczenia techniczne i organizacyjne, zastosowane celem ochrony danych osobowych w DIGICOS. Czyniąc zadość art. 30 RODO, w DIGICOS prowadzone są Rejestry Czynności Przetwarzania (załącznik nr 1 do Polityki).
3. W związku z powyższym kluczowe jest, by wszystkie osoby zatrudnione w DIGICOS, niezależnie od stosunku prawnego regulującego podstawę ich zatrudnienia, zapoznały się i przestrzegały postanowień tego dokumentu. Powyższe znajduje zastosowanie do osób posiadających chociażby przejściowy dostęp do danych, w tym niezależnych podwykonawców oraz osób, które realizują zadania w imieniu podwykonawców.
4. Polityka znajduje zastosowanie do wszelkich operacji, na danych osobowych, jakie mają miejsce w DIGICOS, w tym do:
  - 1) danych osobowych przetwarzanych w systemach informatycznych oraz w tradycyjnej - papierowej formie, a także przechowywanych na wszelkich nośnikach magnetycznych, optycznych, elektronicznych takich jak: zewnętrzny dysk, CD/DVD/Blue-Ray, pamięć USB;
  - 2) danych osobowych przetwarzanych zarówno w zbiorach danych, zestawach oraz pojedynczych informacjach osobowych,
  - 3) informacji dotyczących bezpieczeństwa danych osobowych, w szczególności informacji służących do uwierzytelnienia się w systemach informatycznych, w których mogą występować dane osobowe (loginy i hasła).

Polityka znajduje zastosowanie do wszystkich lokalizacji jak i oddziałów DIGICOS – budynków i pomieszczeń – w których są lub będą przetwarzane dane, ale także do przetwarzania, które odbywa się na urządzeniach mobilnych, takich jak telefony komórkowe lub laptopy.

5. Niniejsza Polityka jest udostępniana w formie elektronicznej bądź w siedzibie DIGICOS, na wniosek osób, które zostały przez nas upoważnione do przetwarzania danych osobowych. Ponadto Polityka jest przekazywana każdorazowo osobie, która takie upoważnienie ma dostać.

#### § 4. ZASADY OGÓLNE PRZETWARZANIA DANYCH OSOBOWYCH

1. DIGICOS, jako Spółka działająca w branży telekomunikacyjnej, współpracuje z wieloma podmiotami na terenie całego kraju. DIGICOS poszukuje nowych klientów oraz zatrudnia pracowników. W związku z powyższym, za kluczowy obszar przetwarzanych danych osobowych można uznać dane pracowników oraz dane kontrahentów. Niniejsza Polityka ma więc zastosowanie dla celu w jakim odbywa się przetwarzania danych osobowych w DIGICOS.
2. Intencją DIGICOS jest, by przetwarzanie danych osobowych odbywało się za aprobatą osób, których dane dotyczą, w sposób transparentny i rzetelny.
3. Wszystkie dane osobowe gromadzone w DIGICOS mogą być przetwarzane wyłącznie w sposób zgodny z przepisami prawa. Dane przetwarzane mogą być jedynie, jeśli spełniona jest jedna z przesłanek wymienionych w art. 6 ust. 1 RODO. DIGICOS przewiduje, iż spośród przesłanek wymienionych w tym przepisie, dane osobowe mogą być przetwarzane najczęściej na podstawie tych wskazanych w literach art. 6 ust. 1 a), b), c) oraz f). Konsekwentnie, jeśli w imieniu DIGICOS przetwarzane są dane osobowe, każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana upewnić się, że występuje co najmniej jedna z tych okoliczności:
  - 1) osoba, której dane dotyczą wyraziła zgodę na takie przetwarzanie danych osobowych,
  - 2) przetwarzanie danych jest niezbędne, w celu wykonania umowy wiążącej DIGICOS z osobą, której dane dotyczą lub w celu zawarcia z nią takiej umowy na jej własne żądanie,
  - 3) przetwarzanie takich danych jest niezbędne, by DIGICOS zrealizowała ciężący na niej obowiązek prawny,
  - 4) istnieje prawnie uzasadniony interes DIGICOS lub innego podmiotu w przetwarzaniu tych danych, wcześniej przeanalizowany i zaakceptowany przez DIGICOS.

Jeśli istnieją wątpliwości, co do tego, czy przetwarzanie znajduje podstawę w którejś z wymienionych przesłanek, należy niezwłocznie poinformować o tym bezpośredniego przełożonego lub Koordynatora ds. danych osobowych (jeśli został powołany).

4. Zbierane dane powinny być merytorycznie poprawne, dlatego należy unikać zbierania danych, o których wiadomo, że są nieprawdziwe i w miarę możliwości należy ustalać dane poprawne. Dążenie do ustalenia poprawnych danych powinno bezwzględnie odbywać się z poszanowaniem praw i prywatności osób, których dane dotyczą oraz z uwzględnieniem zasady minimalizacji danych (nie zbierania przy tym danych dodatkowych).

5. Przy przetwarzaniu wszelkich danych osobowych, poza właściwą podstawą z art. 6 ust. 1 RODO, należy zawsze mieć świadomość celu przetwarzania i ustalić, czy cel jest zgodny z ustaloną podstawą. Odrębne cele przetwarzania wymagają bowiem każdorazowo znalezienia prawidłowej podstawy przetwarzania danych osobowych.
6. Zabronione jest zbieranie jakichkolwiek danych nieistotnych z punktu widzenia celu przetwarzania lub o większym stopniu szczegółowości niż jest to potrzebne dla osiągnięcia tego celu. Jeśli więc dana osoba jest odpowiedzialna za proces zbierania danych w związku z pewnym celem, musi się upewnić, że nie żąda danych, które nie będą niezbędne do osiągnięcia tego celu.
7. Dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania, w tym obejmujących cele DIGICOS takie jak dochodzenie roszczeń, czy obowiązki związane z archiwizacją dokumentów. Po tym okresie dane mogą być przechowywane tylko po uprzedniej ich anonimizacji.
8. Aby uchronić gromadzone przez DIGICOS dane osobowe przed utratą, kradzieżą bądź nieautoryzowanymi zmianami, DIGICOS wdraża szereg zabezpieczeń związanych z ich fizyczną ochroną oraz bezpieczeństwem w sferze informatycznej. Jest obowiązkiem każdej osoby upoważnionej do przetwarzania danych osobowych stosować się do przyjętych przez DIGICOS zasad bezpieczeństwa.
9. Celem zapewnienia systemowego i kompleksowego podejścia do ochrony danych osobowych w DIGICOS, zaleca się powołanie Koordynatora ds. danych osobowych, który to odpowie na wszelkie wątpliwości odnośnie stosowania niniejszej Polityki.
10. DIGICOS działa zgodnie z zasadą uwzględniania prywatności na etapie projektowania oraz prywatności jako ustawienia domyślnego. Te dwie zasady winny znaleźć odzwierciedlenie przy każdym nowym projekcie wdrażanym przez DIGICOS i fakt ten powinien być udokumentowany.
11. W przypadku nowych projektów wdrażanych przez DIGICOS, w tym przede wszystkim, jeśli przewidują one przetwarzanie danych osobowych w sferze elektronicznej, należy ocenić, jak projektowane rozwiązania będą wpływać na prawa i wolności osób, których dane dotyczą. W tym celu, każdorazowo zespół zajmujący się nowym projektem powinien zawierać w swoim składzie osobę, która będzie odpowiedzialna za bieżącą kontrolę tego, jak proponowane przedsięwzięcie wpłynie na bezpieczeństwo danych osobowych, które przetwarzamy, a także tych, które możemy przetwarzać w przyszłości.
12. Zapewnienie prywatności, jako ustawienia domyślnego oznacza, że intencją DIGICOS jest minimalizacja przetwarzanych danych osobowych, a każdorazowe podanie danych osobowych przez osobę, której dane dotyczą, czy wyrażenie przez nią zgody na przetwarzanie tych danych, musi wymagać wyraźnego potwierdzającego działania. Nieodpuszczalna jest sytuacja, kiedy do

zbierania danych o osobie dochodzi bez jej wiedzy czy w sposób, w którym jest ona niepoinformowana o możliwości odmowy podania pewnych danych.

## § 5. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, DIGICOS wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami prawa. Środki te opisane zostały w niniejszej Polityce i w Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych. Środki te będą w razie potrzeby poddawane przeglądowi i uaktualniane. Mechanizmy ochronne służące zapewnieniu bezpieczeństwa danych osobowych zawarte są również w obowiązujących w DIGICOS: Instrukcji Tworzenia i Przechowywania Kopii Zapasowych, Zasadach Bezpiecznego Użytkowania Komputerów Osobistych, Sprzętu Informatycznego oraz Sieci Teleinformatycznej i Instrukcji Bezpieczeństwa Sieci Komputerowej.
2. Zapewnienie bezpieczeństwa danych polega na zagwarantowaniu:
  - 1) **poufności danych**, tj. zapewnieniu, iż jedynie uprawnione osoby posiadać będą dostęp do danych – DIGICOS realizuje to wymaganie poprzez nadawanie upoważnień do przetwarzania danych osobowych - jeśli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych, a w ramach swoich obowiązków powinna takie dane przetwarzać, powinna to niezwłocznie zgłosić bezpośrednio przełożonemu;
  - 2) **integralności danych**, tj. dokładności oraz kompletności danych, jak również metod weryfikacji ich poprawności – DIGICOS realizuje tą wytyczną poprzez wdrożenie systemów informatycznych, które agregują dane i wymagają odpowiedniego stopnia autoryzacji do wykonywania operacji;
  - 3) **rozliczalności działań**, przez co należy rozumieć, że wszystkie działania istotne w zakresie przetwarzania danych zostały zarejestrowane, a w konsekwencji możliwe jest zidentyfikowanie osoby odpowiedzialnej za dokonanie konkretnej operacji na danych – w tym celu wszystkie operacje dokonywane w systemie informatycznym są dokonywane przez indywidualnie określone osoby – należy się upewnić, że używając systemów informatycznych dana osoba korzysta ze swojego własnego loginu i nie udostępnia go innym;
  - 4) **dostępności danych**, czyli zapewnieniu dostępu do danych osobom, których dane dotyczą – DIGICOS wdraża zasady organizacyjne pozwalające osobom, których dane dotyczą wgląd do ich danych w określonym zakresie;
  - 5) **odporności systemów i usług przetwarzania**, czyli przedsięwzięciu działań zmierzających do uniemożliwienia bądź uodpornienia systemów informatycznych lub procesów przetwarzania na ataki z zewnątrz – DIGICOS utrzymuje oprogramowanie zapobiegające nieautoryzowanemu dostępowi do danych, a także podejmuje



działania, aby wszelkie aplikacje, gdzie dane są przetwarzane, były na bieżąco aktualizowane;

- 6) **prawidłowego zarządzania ryzykiem**, tj. przedsięwzięciu działań zmierzających do umożliwienia zidentyfikowania, kontrolowania oraz eliminowania powstającego w związku z przetwarzaniem danych ryzyka naruszenia praw i wolności osób fizycznych – DIGICOS prowadzi okresowe szkolenia dla swojego personelu, aby zapewnić że jest świadomy ryzyk związanych z przetwarzaniem danych osobowych – jeśli dana osoba czuje, że pewne aspekty jej pracy w zakresie, w jakim przetwarza dane osobowe pozostają niejasne, w tym na przykład nie wie, w jaki sposób realizowane są w praktyce postanowienia niniejszej Polityki, powinna skontaktować się z bezpośrednim przełożonym lub Koordynatorem ds. ochrony danych osobowych (jeśli został powołany).
3. Celem zapewnienia bezpieczeństwa danych osobowych wprowadzono mechanizmy ochronne, które wzajemnie się przenikają. Mechanizmami tymi są zabezpieczenia fizyczne, środki sprzętowe, procedury organizacyjne oraz rozwiązania informatyczne.
  4. Zabezpieczenia **fizyczne** obejmują w szczególności:
    - 1) umożliwianie dostępu do danych osobowych tylko osobom, które posiadają ku temu stosowne upoważnienie;
    - 2) przechowywanie fizycznych zbiorów danych w szafkach/pomieszczeniach zamykanych na klucz lub na kod, w tym dotyczy to pomieszczeń w których zlokalizowane są serwery, na których gromadzone są dane w formie elektronicznej; obowiązujące w DIGICOS zasady przechowywania danych są zawarte w Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych i Instrukcji Tworzenia i Przechowywania Kopii Zapasowych;
  5. Środki **sprzętowe** obejmują zwłaszcza:
    - 1) sprzęt wykorzystywany w ramach systemu informatycznego służącego do przetwarzania danych osobowych, zapewniający odpowiednie zabezpieczenia w zakresie dostępu do danych; obowiązujące w DIGICOS zasady bezpiecznego korzystania ze sprzętu zawarte są w Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych, Zasadach Bezpiecznego Użytkowania Komputerów Osobistych, Sprzętu Informatycznego oraz Sieci Teleinformatycznej oraz Instrukcji Bezpieczeństwa Sieci Komputerowej;
    - 2) przechowywanie danych osobowych na serwerach, zapewniających najwyższe standardy zabezpieczenia danych osobowych, podparte odpowiednimi postanowieniami umownymi, które przewidują warunki przechowywania danych przez podmioty zewnętrzne; obowiązujące w DIGICOS zasady przechowywania danych są zawarte w Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych i Instrukcji Tworzenia i Przechowywania Kopii Zapasowych;

- 3) wykorzystanie niszcarki.
6. Procedury **organizacyjne** obejmują w szczególności:
    - a. szkolenia dla pracowników mających dostęp do danych,
    - b. okresowe audyty ochrony danych osobowych,
    - c. przeprowadzanie oceny wpływu na przetwarzanie danych w przypadkach i zgodnie z procedurą opisaną w § 6.
    - d. obowiązek dokładania ciągłych starań mających na celu zapewnienie zgodności ochrony danych z aktualnie obowiązującymi wymaganiami, w tym dostosowywania brzmienia Polityki i Instrukcji do zmieniającego się otoczenia prawnego.
  7. Środki ochrony w ramach **rozwiązań informatycznych** zostały uregulowane w obowiązujących w DIGICOS: Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych, Instrukcji Tworzenia i Przechowywania Kopii Zapasowych, Zasadach Bezpiecznego Użytkowania Komputerów Osobistych, Sprzętu Informatycznego oraz Sieci Teleinformatycznej i Instrukcji Bezpieczeństwa Sieci Komputerowej.

## § 6. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

1. Na dzień wejścia w życie niniejszego dokumentu DIGICOS ocenia, że nie prowadzi procesów przetwarzania danych osobowych, które wymagałyby przeprowadzenia procedury oceny skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO. Obowiązkiem DIGICOS jest jednak na bieżąco badać, czy przesłanki tego przepisu są spełnione, tj. czy istnieje duże prawdopodobieństwo, że prowadzone przez DIGICOS procesy przetwarzania danych osobowych mogą powodować wystąpienie wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, których dane dotyczą.
2. Przed rozpoczęciem nowego procesu przetwarzania danych osobowych lub zmiany procesu istniejącego, DIGICOS jest zobowiązany ustalić, czy nowy proces lub nowy sposób przetwarzania spełnia warunki, o których mowa w punkcie 1 i przez to wymaga przeprowadzenia oceny skutków dla ochrony danych osobowych.
3. Ustalenia tego dokonuje się poprzez zbadanie, czy w danym procesie przetwarzania występują do **co najmniej dwie czynności** z poniższej listy:
  - 1) dokonywana jest ocena lub punktacja osób fizycznych, w tym ich profilowanie lub prognozowanie ich zachowań na podstawie zebranych danych osobowych;
  - 2) podejmowane są automatyczne decyzje mające skutki prawne lub w podobny sposób istotnie wpływające na sytuację osoby, której dane dotyczą;
  - 3) dochodzi do systematycznego monitorowania, przez które rozumie się przetwarzanie danych w celu obserwowania, monitorowania lub kontroli osób, których dane dotyczą;

- 4) występuje przetwarzanie danych wrażliwych – pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, a także przetwarzanie danych dotyczących komunikacji elektronicznej, danych o lokalizacji czy danych finansowych;
  - 5) występuje przetwarzanie danych na dużą skalę – pod względem liczby bezwzględnej osób, procentu populacji, zasięgu terytorialnego przetwarzania;
  - 6) dochodzi do porównywania lub łączenia danych pochodzących z różnych zbiorów danych;
  - 7) występuje przetwarzanie danych osób wymagających szczególnej ochrony np. pracowników, dzieci, pacjentów czy osób starszych;
  - 8) dochodzi do użycia lub stosowania innowacyjnych technologicznych lub organizacyjnych rozwiązań, np. połączenia identyfikacji odciskiem palca oraz mechanizmu rozpoznawania twarzy w celu uzyskania dostępu do pomieszczeń; w zakres takiego przetwarzania wchodzi aplikacje mieszczące się w pojęciu "Internet of things" („Internet Rzeczy”);
  - 9) ma miejsce transgraniczny transfer danych poza Unię Europejską;
  - 10) występuje przetwarzanie danych uniemożliwiający osobom, których dane dotyczą korzystanie z praw (np. monitoring obszarów publicznie dostępnych) lub mające na celu dopuszczenie do korzystania z usługi lub zawarcia umowy.
4. Lista, o której mowa w punkcie 3 powyżej, ma służyć jako wytyczna, nawet bowiem, jeśli z innych niż wymienione tam powodów, osoby odpowiedzialne za wdrożenie nowej metody przetwarzania danych osobowych uznają, iż może rodzić ryzyko naruszenia praw i wolności osób, których dane dotyczą, DIGICOS powinna przeprowadzić ocenę skutków dla ochrony danych osobowych zgodnie z poniższymi postanowieniami.
5. Ocenę skutków dla ochrony danych rozpoczyna zgłoszenie Koordynatorowi ds. ochrony danych osobowych (jeśli został powołany) lub bezpośrednio przełożonemu przez osobę odpowiedzialną za dany projekt lub kierującą działem, potrzeby przeprowadzenia takiej oceny. Brak takiego zgłoszenia może stanowić istotne naruszenie obowiązków osoby koordynującej projekt lub kierującą działem.
6. Koordynator ds. ochrony danych osobowych (jeśli został powołany) lub bezpośredni przełożony następnie decyduje, czy samodzielnie uczestniczyć w procesie oceny, czy też wyznaczyć osobę odpowiedzialną za proces lub w tym zakresie polegać na usługach podmiotu trzeciego (osoba lub podmiot tak wyznaczony zwani dalej łącznie: **Koordynator DPIA**) .
7. Niezależnie od wyboru, Koordynator DPIA zbiera informacje o projekcie, aby ustalić realne zagrożenia dla przetwarzanych danych osobowych, zbadać, jak te ryzyka mają być ograniczane i czy takie ograniczenia są skuteczne. Wszystkie osoby zaangażowane w projekt mają obowiązek współpracować z Koordynatorem DPIA, to jest udzielać mu informacji o

merytorycznych założeniach projektu, które będą niezbędne by Koordynator DPIA wykonywał swoje obowiązki. Metodologia prac winna opierać się na kryteriach Grupy Roboczej Artykułu 29, które stanowią Załącznik nr 2 do Polityki.

8. Koordynator DPIA sporządza pisemny raport ze swoich prac, który obejmuje co najmniej:
  - 1) opis planowanych operacji przetwarzania i celów przetwarzania z rozróżnieniem na możliwe warianty projektu, jeśli są rozważane;
  - 2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne;
  - 3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz źródeł ryzyka;
  - 4) ocenę prawdopodobieństwa wystąpienia tego ryzyka;
  - 5) środki planowane w celu:
    - a. zaradzenia ryzyku;
    - b. wykazania przestrzegania przepisów, w tym RODO oraz niniejszej Polityki;
  - 6) ocenę, czy środki są skuteczne i wystarczające, by te cele osiągnąć, z uwzględnieniem indywidualnej oceny dla różnych wariantów, projektu, jeśli są rozważane.
9. Raport jest zatwierdzany przez Koordynatora ds. ochrony danych osobowych (jeśli został powołany) lub przez bezpośredniego przełożonego Koordynatora DPIA. W przypadku uznania, że raport pozwala przyjąć, iż planowane środki są wystarczające, by zabezpieczyć prawa i wolności osób fizycznych w procesie przetwarzania, a także zapewnić zgodność z przepisami i niniejszą Polityką, proces może zostać wdrożony. W przeciwnym wypadku zaleca się zamknięcie projektu, a w szczególnie uzasadnionych przypadkach podjąć procedurę konsultacji z organem nadzoru, o której mowa w art. 36 RODO.

## **§ 7. ORGANIZACJA PRACY PRZY PRZETWARZANIU DANYCH**

1. Każdy pracownik lub inna osoba dopuszczona do przetwarzania danych osobowych, których DIGICOS jest administratorem, jest zobowiązana upewnić się, że zapoznała się zasadami dotyczącymi bezpieczeństwa danych osobowych, a także, że otrzymała stosowne upoważnienia do przetwarzania tych danych. Upoważnienia może przyznawać ADO lub osoba posiadająca pełnomocnictwo wydane przez ADO i, co do zasady, powinny być zgodne ze wzorem upoważnienia określonym w Załączniku nr 3 do Polityki. Upoważnienie może mieć formę pisemną, jak i elektroniczną.
2. DIGICOS prowadzi wykaz osób uprawnionych do przetwarzania danych osobowych zgodnie z Załącznikiem nr 4. Osoby upoważnione nie są wykreślane z wykazu po ustaniu upoważnienia, a jedynie odnotowuje się w nim datę wygaśnięcia tego upoważnienia.
3. Każda osoba przetwarzająca dane osobowe, których administratorem jest DIGICOS, w czasie ich przetwarzania jest odpowiedzialna za ich bezpieczeństwo i w tym celu powinna ona

dokładać wszelkich starań, celem uniemożliwienia wglądu bądź zmiany przetwarzanych danych przez osoby do tego nieupoważnione.

4. Osoby dopuszczone do przetwarzania danych są zobowiązane do zachowania w tajemnicy przetwarzanych danych osobowych.
5. Wszystkie osoby, o których mowa w punkcie 1 są zobowiązane do stosowania zasady „czystego biurka”. Oznacza to, że po zakończonej pracy lub przed opuszczeniem stanowiska pracy na dłuższy czas należy upewnić się, że:
  - 1) na stanowisku roboczym nie pozostały niezabezpieczone dokumenty z danymi osobowymi,
  - 2) szafy lub pomieszczenia, w których przechowywane są dane osobowe zostały zamknięte w sposób uniemożliwiający dostęp osób, które nie są upoważnione do przetwarzania danego zakresu danych,
  - 3) komputer został doprowadzony do stanu, który przed wzbudzeniem będzie wymagał podania indywidualnego hasła użytkownika.
6. W miarę możliwości monitor komputera, na którym przetwarzane są dane osobowe powinien być ustawiony w ten sposób, by osoby, które nie mają dostępu do przetwarzania danego zakresu danych, w tym szczególnie osoby postronne, nie miały bezpośredniej możliwości obserwowania aktywności wykonywanej na tym monitorze.
7. W zakresie, w jakim jest to możliwe, pomieszczenia lub miejsca, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych.
8. Wszelkie procesy przetwarzania danych osobowych, które odbywają się w DIGICOS powinny znaleźć odzwierciedlenie w Rejestrze Czynności Przetwarzania. Dlatego też zawsze należy się upewnić, że dokonywane operacje są objęte tym rejestrem. Jeśli występują jakiegokolwiek wątpliwości w tym zakresie, należy skontaktować się z Koordynatorem ds. ochrony danych osobowych (jeśli został powołany) lub z bezpośrednim przełożonym.

## **§ 8. KONTAKT Z OSOBAMI, KTÓRYCH DANE DOTYCZĄ**

1. Celem DIGICOS jest, by wszelka komunikacja z osobami, których dane dotyczą odbywała się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności, gdy informacje są kierowane do dziecka.

2. Informacji osobie, której dane dotyczą należy udzielać na piśmie lub elektronicznie, w zależności od jej wyboru. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość tej osoby.
3. W przypadku zbierania danych osobowych bezpośrednio od osób, których dane dotyczą (a więc na przykład: na formularzach, umowach, kwestionariuszach, drukach, zarówno papierowych, jak i elektronicznych), należy umieszczać na nich klauzulę informacyjną, jeśli osoba ta nie dysponuje tymi danymi. Klauzula informacyjna winna być łatwo dostępna, widoczna, wyodrębniona od innych oświadczeń i zawierać:
  - 1) pełną nazwę i adres DIGICOS,
  - 2) imię, nazwisko i adres Inspektora Ochrony Danych, jeśli został ustanowiony,
  - 3) cel zbierania danych oraz podstawę ich przetwarzania, a jeśli podstawą jest prawnie uzasadniony interes Spółki (art. 6 ust. 1 lit. f) RODO), również informację na temat tego uzasadnionego interesu,
  - 4) okres, przez który dane osobowe będą przetwarzane, a jeśli nie jest to możliwe, kryteria ustalenia tego okresu,
  - 5) nazwy lub kategorie podmiotów, którym dane mogą być przekazywane,
  - 6) informacje o prawie do żądania od DIGICOS dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także o prawie do przenoszenia danych, żądania ich usunięcia lub wniesienia sprzeciwu w sytuacjach prawem przewidzianych,
  - 7) jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
  - 8) informacje o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,
  - 9) informacje czy podanie określonych danych jest obowiązkowe, czy też dobrowolne,
  - 10) w sytuacji, gdy podanie danych jest dobrowolne, informację czy jest ono niezbędne do podjęcia przez Spółkę określonych czynności, w tym, jakie są konsekwencje niepodania danych,
  - 11) w sytuacji, gdy podanie danych jest obowiązkowe, przepis prawa, który konstytuuje taki obowiązek,
  - 12) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (jeśli dotyczy).
4. W przypadku zbierania danych osobowych z innych źródeł (nie od osoby, której dane dotyczą), bezpośrednio po utrwaleniu zebranych danych, nie później jednak niż w terminie 1 miesiąca od ich utrwalenia lub do momentu pierwszej komunikacji z osobą, której dane dotyczą

(którekolwiek nastąpi wcześniej), należy udzielić tej osobie informacji, o których mowa w ust. 3, z wyłączeniem pkt 9-11, a ponadto również informacji o:

- 1) zakresie przetwarzanych danych (ich kategoriach);
  - 2) źródle, z którego dane zostały pozyskane, w tym, czy pochodzą one ze źródeł powszechnie dostępnych;
  - 3) prawach do wniesienia sprzeciwu w odniesieniu do przetwarzania danych osobowych, w zakresie wynikającym z art. 21 RODO.
5. Udzielenie informacji, o których mowa w punkcie 4 powyżej, nie jest obowiązkowe, jeżeli:
- 1) osoba, której dane dotyczą dysponuje już tymi informacjami,
  - 2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku,
  - 3) pozyskiwanie lub ujawnianie danych jest wyraźnie uregulowane prawem,
  - 4) DIGICOS jest w tym zakresie związana obowiązkiem zachowania w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej.
6. Jeżeli DIGICOS planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje ona osobę, której dane dotyczą, o tym innym celu. Powyższe nie może uchybiać postanowieniom dotyczącym istnienia podstawy prawnej dla każdego przetwarzania.
7. Do obowiązków każdej osoby dopuszczonej do przetwarzania danych należy upewnienie się, że kontakt z osobą, której dane dotyczą odbywa się zgodnie z postanowieniami niniejszego paragrafu. Jeśli więc istnieją wątpliwości, czy osoby, których dane są przetwarzane otrzymały powyższe informacje, należy poinformować o tym fakcie bezpośredniego przełożonego lub Koordynatora ds. ochrony danych osobowych (jeśli został powołany).

## **§ 9. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ**

1. Obowiązkiem DIGICOS jest zapewnić osobom, których dane dotyczą przestrzegania ich praw, przysługujących w związku z przetwarzaniem ich danych osobowych. Realizacja praw osób spoczywa na kierownikach poszczególnych działów, którzy decydują o sposobie załatwienia wniosków osób fizycznych w tym zakresie, jednak każda osoba, która przetwarza dane osobowe może spotkać się z takim wnioskiem, stąd też ważne, by zapoznać się z prawami, jakie osoby, których dane dotyczą mogą wykonywać.
2. Niniejszy paragraf opisuje kluczowe elementy związane z wykonywaniem praw osób, których dane dotyczą, jednak w przypadku realizacji takich praw przez te osoby wobec DIGICOS, osoby odpowiedzialne za ich realizację winny bezwzględnie stosować przepisy art. 16-22 RODO.



3. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:
  - 1) uzyskania wyczerpującej informacji o przetwarzaniu danych, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
  - 2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych,
  - 3) uzyskania informacji, od kiedy przetwarza się dane jej dotyczące, do kiedy planowane jest ich przetwarzanie oraz podania w powszechnie zrozumiałej formie treści tych danych,
  - 4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że ADO jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej,
  - 5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
  - 6) uzyskania informacji o prawie wniesienia skargi do organu nadzorczego,
  - 7) uzyskania informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,
  - 8) żądania sprostowania danych nieprawidłowych,
  - 9) żądania usunięcia dotyczących jej danych, jeśli wystąpiły okoliczności z art. 17 ust. 1 RODO (prawo do bycia zapomnianym),
  - 10) żądania ograniczenia przetwarzania, w przypadkach opisanych w art. 18 ust. 1 RODO,
  - 11) przenoszenia danych zgodnie z art. 20 RODO,
  - 12) gdy przetwarzanie danych odbywa się ze względu na prawnie uzasadniony interes DIGICOS, wniesienia:
    - a. pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,
    - b. sprzeciwu wobec przetwarzania jej danych, gdy ADO zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu ADO.
4. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź musi nastąpić w terminie 30 dni od daty jego otrzymania. Odpowiedź może być udzielona na piśmie lub w innej formie wskazanej przez wnioskodawcę.
5. Osoba, której dane dotyczą, może się zwracać z wnioskiem o udzielenie informacji, nie częściej niż raz na 6 miesięcy. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, DIGICOS pobierze opłatę w rozsądnej wysokości, wynikającej z kosztów administracyjnych.



6. W sytuacji wniesienia przez osobę sprzeciwu wobec przetwarzania jej danych, informacja o wniesieniu sprzeciwu przekazywana jest do ADO, Koordynatora ds. ochrony danych osobowych (jeśli został powołany) lub IOD (jeśli został powołany). Dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. ADO może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.
7. Osoba, której dane dotyczą, ma prawo żądania od DIGICOS niezwłocznego usunięcia dotyczących jej danych osobowych, a DIGICOS ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeśli spełnione są przesłanki wystosowania takiego żądania. Jeżeli w toku działalności upubliczni ona takie dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Nie dotyczy to przekazania danych w celu wykonania przepisów prawa lub dochodzenia roszczeń.
8. Realizacja prawa do przenoszenia danych może mieć miejsce jedynie w przypadku przetwarzania danych na podstawie zgody lub w celu wykonania umowy. W takim przypadku osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu dane osobowe jej dotyczące, które dostarczyła Spółce.

## **§ 10. ZADANIA OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ DANYCH**

1. Za bezpieczeństwo danych odpowiadają:
  - 1) Administrator Danych Osobowych,
  - 2) Koordynator ds. ochrony danych osobowych, jeśli został powołany,
  - 3) Administrator Systemu Informatycznego,
  - 4) pracownicy upoważnieni do przetwarzania danych osobowych,
  - 5) IOD, jeśli został powołany.
2. Zadania Koordynatora ds. ochrony danych osobowych obejmują:
  - 1) uczestniczenie w tworzeniu, wdrażaniu i interpretowaniu dokumentacji ochrony danych osobowych standardów, zaleceń oraz procedur, dotyczących przetwarzania danych osobowych,
  - 2) koordynowanie działań w zakresie ochrony danych osobowych,
  - 3) monitorowanie przestrzegania przepisów prawa w zakresie danych osobowych, a także Polityki i Instrukcji,

- 4) informowanie ADO oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów prawa,
- 5) ścisłą współpracę z ASI w zakresie ustalenia zasad i nadzoru nad poprawnością przetwarzania danych osobowych w systemach informatycznych,
- 6) zapoznanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami o ochronie danych osobowych poprzez przeprowadzenie szkoleń,
- 7) prowadzenie Rejestru Czynności Przetwarzania,
- 8) opiniowanie umów dotyczących powierzenia podmiotom trzecim przetwarzania danych osobowych,
- 9) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń,
- 10) uczestnictwo w ocenie skutków dla ochrony danych osobowych,
- 11) kontakt z organem nadzoru,
- 12) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO.

### 3. Zadania ASI obejmują:

- 1) rejestrowanie i wyrejestrowywanie użytkowników systemu,
- 2) dokonywanie zmiany uprawnień użytkowników systemu,
- 3) przestrzeganie opracowanych dla systemu procedur bezpieczeństwa,
- 4) utrzymanie systemu informatycznego w sprawności technicznej,
- 5) przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe,
- 6) konfigurowanie urządzeń i oprogramowania służących do przetwarzania danych osobowych, według zapotrzebowania,
- 7) aktualizowanie i konfigurowanie oprogramowania antywirusowego i antyspamowego,
- 8) reagowanie na naruszenia bezpieczeństwa i usuwanie ich przyczyn i skutków,
- 9) nadzorowanie właściwego użytkowania oraz serwisowania urządzeń i oprogramowania,
- 10) prowadzenie dziennika pracy systemu, który zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego, w szczególności w przypadku awarii – opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski,
- 11) w przypadku konserwacji systemu – opis podjętych działań, wnioski,

- 12) wykonywanie kopii bezpieczeństwa baz danych, w których przetwarzane są dane osobowe oraz systemów informatycznych,
  - 13) prowadzenie dokumentacji technicznej systemów,
  - 14) informowanie ADO lub Koordynatora ds. ochrony danych osobowych (jeśli został powołany) o wszelkich zdarzeniach związanych lub mogących mieć wpływ na bezpieczeństwo systemu teleinformatycznego.
4. Pracownicy, niezależnie od stosunku prawnego regulującego podstawę ich zatrudnienia, zobowiązani są do:
- 1) zachowania w tajemnicy danych osobowych, do których mają dostęp, a także sposobów zabezpieczenia tych danych, zarówno w trakcie jak i po ustaniu tego stosunku,
  - 2) przestrzegania przepisów wewnętrznych obowiązujących w DIGICOS wiążących się z ochroną danych osobowych, w tym Polityki i Instrukcji,
  - 3) zgłaszania zauważonych incydentów bezpieczeństwa związanych z ochroną danych osobowych.

## **§ 11. ODBIORCY DANYCH**

1. Za odbiorców danych w rozumieniu niniejszej Polityki należy uznać wszystkie podmioty, które otrzymują od nas dane osobowe, w tym w szczególności:
  - 1) podmioty przetwarzające - podmioty, które nie decydują samodzielnie o celach i środkach przetwarzania danych, ale wykonują pewne czynności przetwarzania danych na zlecenie i w wykonaniu celów DIGICOS, w oparciu o art. 28 RODO,
  - 2) podmioty trzecie – inni odbiorcy danych, w tym inni administratorzy danych, którzy otrzymują dane osobowe w oparciu o przepisy art. 6 ust. 1 RODO.
2. Powierzenie przetwarzania danych osobowych podmiotowi przetwarzającemu wymaga zawarcia umowy w formie pisemnej, określającej w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora zgodnie z art. 28 RODO.
3. DIGICOS może korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przewidziane przepisami prawa i chroniło prawa osób, których dane dotyczą. Do osoby odpowiedzialnej za zawarcie umowy z takim podmiotem należy dołożenie starań, celem ustalenia, że podmiot ten spełnia powyższe warunki.

4. Dane osobowe przetwarzane przez DIGICOS nie mogą być udostępniane podmiotom trzecim, chyba że istnieje podstawa prawna dla udostępnienia tych danych osobowych, a w szczególności osoba, której dane dotyczą wyraziła zgodę na udostępnienie jej danych podmiotowi trzeciemu lub istnieje przepis prawa nakazujący takie udostępnienie.
5. Możliwość przekazywania lub udostępniania danych osobowych podmiotom spoza Unii Europejskiej jest szczególnie ograniczona. W każdym przypadku takie przekazanie wymaga przeanalizowania jego dopuszczalności na gruncie przepisów art. 44-50 RODO.
6. Jest niezmiernie ważne, by każda osoba przetwarzająca dane osobowe w DIGICOS przekazywała dane odbiorcom danym jedynie wówczas, gdy takie przekazanie spełnia wymogi niniejszej Polityki. Sam proces przekazywania powinien być każdorazowo uwzględniony w Rejestrze Czynności Przetwarzania. Jeśli więc należy przekazać dane podmiotowi przetwarzającemu lub podmiotowi trzeciemu, a taka możliwość nie wynika z Rejestru Czynności Przetwarzania, przed przekazaniem danych osobowych należy skonsultować to z bezpośrednim przełożonym lub Koordynatorem ds. ochrony danych osobowych (jeśli został powołany).

## **§ 12. POSTĘPOWANIE Z INCYDENTAMI**

1. Incydem jest każde naruszeniem zasad ochrony danych osobowych, w szczególności:
  - 1) nieuprawniony dostęp lub próba dostępu do danych osobowych,
  - 2) udostępnianie danych osobom nieupoważnionym,
  - 3) przetwarzanie danych przez osoby nieupoważnione,
  - 4) utrata danych zapisanych na kopiach zapasowych,
  - 5) naruszenie poufności, integralności lub dostępności danych.
2. Każdy pracownik DIGICOS, niezależnie od stosunku prawnego regulującego podstawę jego zatrudnienia, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować o tym bezpośredniego przełożonego lub Koordynatora ds. ochrony danych osobowych (jeśli został powołany), w terminie nie dłuższym niż 24 h od wystąpienia incydentu, a w przypadku jeśli incydent wystąpi w przeddzień dnia wolnego od pracy, jeszcze w tym samym dniu.
3. W przypadku stwierdzenia incydentu (naruszenia), Koordynator ds. ochrony danych osobowych (jeśli został powołany) lub bezpośredni przełożony prowadzi postępowanie wyjaśniające, w toku którego:
  - 1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,

- 2) zabezpiecza ewentualne dowody,
  - 3) ustala osoby odpowiedzialne za naruszenie,
  - 4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
  - 5) inicjuje działania dyscyplinarne,
  - 6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
  - 7) dokumentuje prowadzone postępowania,
  - 8) sporządza raport z incydentu.
4. Tryb postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego określa Instrukcja.
  5. Po otrzymaniu informacji o wystąpieniu incydentu Koordynator ds. ochrony danych osobowych (jeśli został powołany) lub bezpośredni przełożony ocenia, czy incydent ten skutkował ryzykiem naruszenia praw lub wolności osób fizycznych i raportuje swoje wnioski do Zarządu. W przypadku stwierdzenia prawdopodobieństwa takiego ryzyka, w terminie nie dłuższym niż 72 h od wystąpienia incydentu, DIGICOS zgłasza to naruszenie Prezesowi Urzędu Ochrony Danych Osobowych.
  6. ADO prowadzi rejestr incydentów, zawierający w szczególności opis okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

### **§ 13. ODPOWIEDZIALNOŚĆ**

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami określonymi w art. 83 RODO, art. 101 Ustawy oraz w art. 266 - 269 Kodeksu karnego.
2. W związku z powyższym wszelkie incydenty związane z naruszeniem zasad ochrony danych osobowych mogą skutkować zarówno odpowiedzialnością bezpośrednią osób, które do incydentu dopuściły, jak i odpowiedzialnością finansową DIGICOS sięgającą nawet 20 mln EUR.
3. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 1, naruszenie zasad ochrony danych osobowych obowiązujących w DIGICOS, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

**ZAŁĄCZNIK NR 1. Rejestr Czynności Przetwarzania**

[EXCEL]

## **ZAŁĄCZNIK NR 2. Wytyczne dotyczące oceny skutków dla ochrony danych**

### 1. Zapewniono systematyczny opis operacji przetwarzania (art. 35 ust. 7 lit. a RODO):

- uwzględniono charakter, zakres, kontekst i cele przetwarzania (motyw 90);
- w rejestrze zamieszczono dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych;
- przedstawiono funkcjonalny opis operacji przetwarzania;
- zidentyfikowano zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań);
- uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania (art. 35 ust. 8);

### 2. Oceniono niezbędność oraz proporcjonalność (art. 35 ust. 7 lit. b)):

- wskazano środki, których podjęcie jest planowane w celu zapewnienia przestrzegania rozporządzenia (art. 35 ust. 7 lit. d) i motyw 90), uwzględniając:
  - a) środki przyczyniające się do proporcjonalności i niezbędności przetwarzania, z uwzględnieniem następujących aspektów:
    - /konkretne, wyraźne i prawnie uzasadnione cele (art. 5 ust. 1 lit. b));
    - /zgodność przetwarzania z prawem (art. 6);
    - /dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c));
    - /ograniczony czas przechowywania (art. 5 ust. 1 lit. e));
  - b) środki przyczyniające się do zachowania praw osób, których dane dotyczą:
    - /poinformowanie osoby, której dane dotyczą (art. 12, 13 i 14);
    - /prawo dostępu i prawo do przenoszenia danych (art. 15 i 20);
    - /prawo do sprostowania i do usunięcia danych (art. 16, 17 i 19);
    - /prawo do sprzeciwu i prawo do ograniczenia przetwarzania (art. 18, 19 i 21);
    - /relacje z podmiotem przetwarzającym (art. 28);
    - /zabezpieczenia przy międzynarodowym przekazywaniu danych (rozdział V);
    - /uprzednie konsultacje (art. 36);

### 3. Przeprowadzono działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą (art. 35 ust. 7 lit. c)):

- uwzględniono źródło, charakter, specyfikę i powagę ryzyka (por. motyw 84), czy konkretniej, w przypadku każdego rodzaju ryzyka (bezprawnego dostępu, niepożądanego zmiany i zniknięcia danych), z punktu widzenia osób, których dane dotyczą:
  - a) uwzględniono źródła ryzyka (motyw 90);
  - b) zidentyfikowano możliwe skutki dla praw i wolności osób, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych;
  - c) zidentyfikowano zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych;
  - d) oszacowano prawdopodobieństwo i powagę (motyw 90);
- określono środki, których podjęcie jest planowane w celu zaradzenia ryzyku (art. 35 ust. 7 lit. d) i motyw 90);

### 4. Zaangażowano zainteresowane strony:

- skonsultowano się z inspektorem ochrony danych w celu uzyskania zalecenia (art. 35 ust. 2);
- w stosownych przypadkach zasięgnięto opinii osób, których dane dotyczą, lub ich przedstawicieli (art. 35 ust. 9).

### ZAŁĄCZNIK NR 3. Wzór upoważnienia

#### Upoważnienie do przetwarzania danych

#### UPOWAŻNIENIE Nr .....

Działając w imieniu **DIGICOS S.A.** (dalej: Spółka) upoważniam:

**Pana/Panią** .....

do przetwarzania danych osobowych, których Spółka jest administratorem w następującym zakresie .....

w celu .....

.....,

**Upoważnienie wydano w dniu** .....

**Upoważnienie traci ważność z dniem rozwiązania umowy będącej podstawą zatrudnienia w DIGICOS S.A. lub z dniem odwołania upoważnienia.**

**Nr identyfikatora** .....

*/jeżeli dane przetwarzane są w systemie informatycznym/*

.....

Data i podpis

#### **Pouczenie**

Osoba, która została upoważniona oświadcza, iż zapoznała się z dokumentacją wewnętrzną dotyczącą ochrony danych osobowych obowiązującą w DIGICOS S.A. i zobowiązuje się do przestrzegania jej postanowień, w szczególności obowiązana jest zachować w tajemnicy wobec osób nieuprawnionych przetwarzane dane osobowe oraz sposób ich zabezpieczenia.

Powyższe przyjmuję do wiadomości i wykonania:

.....

Data i podpis



**ZAŁĄCZNIK NR 4. Rejestr upoważnionych**

Lp.	Imię nazwisko	Zakres przydzielonych uprawnień	Data przyznania uprawnień	Data ustania uprawnień
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				