Polityka Ochrony Danych Osobowych

w Instytucie Doskonałości Strategicznej Sp. z o.o.

Toruń, 25.05.2018

Uwzględniając obowiązki wynikające z art. 25 oraz art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1), celem zapewnienia, że dane osobowe w Instytucie Doskonałości Strategicznej Sp. z o.o. (IDS) są przetwarzane i zabezpieczone zgodnie z postanowieniami prawa poprzez wdrożenia odpowiednich środków technicznych i organizacyjnych, zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń.

§ 1 Postanowienia Ogólne

1.1. Polityka określa zasady przetwarzania oraz zabezpieczania danych osobowych w IDS, celem zapewnienia zgodności przetwarzania z wymaganiami RODO oraz przepisami obowiązującego prawa krajowego w zakresie przetwarzania i danych osobowych. Polityka stanowi zbiór oraz podstawę wdrażanych w IDS rozwiązań, procedur oraz zasad ochrony danych osobowych. Polityka zawiera: opis zasad ochrony danych obowiązujących w IDS, zbiór procedur, instrukcji i regulacji szczegółowych dotyczących przetwarzania Danych osobowych w IDS, dotyczących poszczególnych obszarów z zakresu ochrony danych osobowych; stanowiących załączniki do Polityki.

1.2. Polityka i zawarte w niej zapisy obowiązują wszystkich pracowników oraz instytucje współpracujące z IDS. Za przestrzeganie i utrzymanie postanowień Polityki odpowiedzialni są:

- kadra zarządzająca,
- komórki organizacyjne wszystkie, w których przetwarzane są dane osobowe;
- pracownicy.

1.3. Dla skutecznej realizacji Polityki, uwzględniając zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia IDS zapewnia:

- wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania danych osobowych z wymogami prawa oraz niezbędne zabezpieczenie przetwarzanych danych osobowych;
- stałe monitorowanie zgodności przetwarzania danych osobowych z wymogami prawa;
- nadzór nad przetwarzaniem danych osobowych.

1.4. Nadzór nad przestrzeganiem postanowień polityki zapewnia Zarząd IDS.

1.5. IDS dba o zgodność postępowania kontrahentów IDS z postanowieniami Polityki w odpowiednim zakresie we wszystkich sytuacjach, w których dochodzi do przekazania tym podmiotom danych osobowych.

1.6. Polityka jest przechowywana i udostępniana w wersji papierowej oraz elektronicznej w siedzibie IDS. Politykę udostępnia się wszystkim osobom upoważnionym do przetwarzania danych osobowych celem zapewnienia osobom upoważnionym należytej wiedzy oraz informacji na temat zasad i wymogów dotyczących przetwarzania Danych osobowych. Polityka ochrony danych osobowych może być udostępniona również osobom zainteresowanym, w szczególności osobom fizycznym, których dane dotyczą – na ich wniosek.

§ 2 Słownik pojęć

2.1. Polityka – oznacza niniejszy dokument wraz ze wszystkimi ewentualnymi Załącznikami;

2.2. Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, takie jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy pozwalające w sposób jednoznaczny zidentyfikować osobę fizyczną zgodnie z art. 4 pkt 1 RODO;

2.3. RODO – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1);

2.4. Osoba upoważniona – oznacza osobę upoważnioną przez Instytut Doskonałości Strategicznej Sp. z o.o. do przetwarzania danych osobowych w danym zakresie;

2.5. Przetwarzanie – oznacza czynność lub zestaw czynności wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. Do tych czynności należy między innymi 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, o których mowa w art. 4 pkt 2 RODO;

2.6. Zbiór danych – oznacza każdy uporządkowany zestaw danych osobowych;

2.7. Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu IDS [np. serwis IT, Serwis monitoringu, zewnętrzna księgowość];

2.8. Rejestr – oznacza Rejestr Czynności Przetwarzania Danych Osobowych w IDS;

2.9. Uwierzytelnienie – oznacza działanie, którego celem jest weryfikacja deklarowanej tożsamości Użytkownika;

2.10. IDS – oznacza Instytut Doskonałości Strategicznej Sp. z o.o.;

2.11. Pracownicy – oznaczają zarówno osoby zatrudnione w IDS na podstawie stosunku pracy, jak również osoby fizyczne współpracujące z IDS na podstawie Umowy cywilnoprawnej;

2.12. Dane wrażliwe – oznaczają Dane osobowe, o których mowa w art. 9 RODO – dane tego typu mogą znajdować się wyłącznie w dziale księgowości i w biurze rachunkowym . W dziel księgowości znajdują się wylanie archiwalne teczki pracowników. Teczki aktualnie zatrudnionych są przechowywane przez biuro księgowe.

§ 3 Dane osobowe

3.1. IDS przetwarza Dane osobowe gromadzone w zbiorach danych. Zbiory danych przetwarzane w IDS określa Załącznik nr 1 do Polityki.

3.2. IDS nie podejmuje czynności przetwarzania, które mogłyby wiązać się z istotnym ryzykiem naruszenia praw i wolności osób, których dane osobowe dotyczą. W przypadku planowania podjęcia czynności, o których mowa w zdaniu poprzedzającym IDS obligatoryjnie przeprowadza uprzednią ocenę skutków przetwarzania, o których mowa w art. 35 RODO.

3.3. Dane osobowe domyślnie przetwarzane są na terenie obejmującym pomieszczenia biurowe IDS. Dodatkowy obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym w zdaniu poprzedzającym oraz pomieszczenia biurowe firmy prowadzącej księgi rachunkowe IDS.

§ 4 Podstawowe zasady ochrony Danych osobowych

4.1. IDS stosuje środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.

4.2. Osoby upoważnione oraz wszystkie inne osoby, którym udostępnia się dane osobowe przetwarzane w IDS zobowiązane są do przetwarzania danych osobowych zgodnie z wymogami prawa oraz postanowieniami polityki i procedur wewnętrznych związanych z Przetwarzaniem Danych osobowych.

(4.2.i) Przy zatrudnianiu Pracowników oraz w trakcie zatrudnienia IDS zapewnia, że: pracownicy przed przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad Przetwarzania i ochrony Danych osobowych. Każdy z Pracowników zostaje upoważniony na piśmie do Przetwarzania Danych osobowych w niezbędnym zakresie (a wraz z końcem współpracy otrzymuje odwołanie upoważnienia), zgodnie z wzorem stanowiącym Załączniki nr 2 do Polityki, przy czym Pracownicy zobowiązani są w szczególności do:

- ścisłego przestrzegania zakresu upoważnienia;
- przestrzegania wymogów prawa oraz postanowień Polityki w zakresie przetwarzania;
- zachowania w tajemnicy Danych osobowych;
- niezwłocznego zgłaszania osobom zarządzającym wszelkich incydentów związanych z naruszeniem bezpieczeństwa Danych osobowych.

4.3. IDS dba, aby Dane Osobowe były:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
- adekwatnie to jest ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
- prawidłowe i w razie potrzeby uaktualniane, wszystkie dane które są nieprawidłowe w świetle celów ich przetwarzania zostają niezwłocznie usunięte lub sprostowane;
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są pozyskane;;
- 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.

4.4. Przetwarzając dane osobowe IDS opiera się na następujących zasadach:

- legalności – dbałość o ochronę prywatności i przetwarzanie Danych osobowych zgodnie z wymogami prawa;

- bezpieczeństwa − zapewnienie odpowiedniego poziomu bezpieczeństwa Danych osobowych poprzez podejmowanie stałych działań doskonalących w tym zakresie;
- zachowania prawa jednostki – IDS umożliwia osobom, których Dane osobowe są przetwarzane, wykonywanie swoich praw i prawa te realizuje;
- rozliczalności – zapewnienie należytego udokumentowania sposobu spełniania obowiązków w zakresie ochrony danych osobowych.

§ 5 System ochrony danych osobowych

5.1. IDS zapewnia zgodność Przetwarzania Danych osobowych z wymogami prawa poprzez zaprojektowanie, wprowadzenie i utrzymywanie Systemu ochrony danych osobowych. Na System składają się środki organizacyjne oraz środki techniczne ochrony, adekwatne do poziomu ryzyka zidentyfikowanego dla poszczególnych Zbiorów danych oraz kategorii danych. System składa się z następujących środków:

- ograniczenie dostępu do pomieszczeń, w których przetwarzane są Dane osobowe, jedynie do osób upoważnionych oraz zapewnienie, że inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania Danych osobowych wyłącznie w towarzystwie osoby upoważnionej;
- zamykanie pomieszczeń tworzących obszar przetwarzania danych na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osobom trzecim;
- zapewnienie zabezpieczenia obszaru przetwarzania danych przed czynnikami losowymi, takimi jak pożar lub powódź;
- wykorzystywanie zamykanych szafek, szuflad lub innych środków technicznych uniemożliwiających osobom niepowołanym dostęp do przechowywanych w nich Danych osobowych;
- wdrożenie zasady tzw. czystego biurka;
- zapewnienie skutecznego usuwania lub niszczenia dokumentów zawierających Dane osobowe, w sposób uniemożliwiający ich późniejsze odtworzenie;
- zapewnienie bezpieczeństwa sprzętowego i informatycznego, obejmującego ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz, zapewnienie aktualności stosowanego oprogramowania, zabezpieczenie sprzętu komputerowego wykorzystywanego w IDS przed złośliwym oprogramowaniem, zapewnienie stałego i częstotliwego sporządzania kopii zapasowych danych przechowywanych na komputerach, ograniczenie dostępu do sprzętu komputerowego poprzez stosowanie reguł Uwierzytelniania;
- przeprowadzanie analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
- monitorowanie zmian w zakresie procesów przetwarzania Danych osobowych w IDS oraz na bieżąco zarządza zmianami mającymi wpływ na ochronę Danych osobowych.

§ 6 Rejestr czynności przetwarzania Danych osobowych

6.1. Rejestr obejmuje kategorie czynności przetwarzania Danych osobowych w IDS. Za pośrednictwem Rejestru, IDS dokumentuje czynności przetwarzania Danych osobowych oraz

inwentaryzuje i monitoruje sposób, w jaki wykorzystuje się Dane osobowe. Rejestr stanowi Załącznik nr 3 do Polityki.

6.2. Za pośrednictwem Rejestru, w szczególności poprzez wskazanie w Rejestrze ogólnych środków ochrony Danych osobowych objętych wyodrębnioną czynnością przetwarzania, IDS wykazuje również zgodność przetwarzania Danych osobowych z wymogami prawa.

6.3. W Rejestrze, dla każdej zidentyfikowanej kategorii czynności przetwarzania Danych osobowych, odnotowuje się co najmniej:

- nazwę czynności;
- cel przetwarzania;
- opis kategorii osób, których Dane osobowe przetwarzane są w ramach danej czynności;
- opis kategorii Danych osobowych przetwarzanych w ramach danej czynności;
- podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu
- opis kategorii odbiorców danych, w tym Podmiotów przetwarzających,
- informację o ewentualnym przekazaniu Danych osobowych poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;
- ogólny opis technicznych i organizacyjnych środków ochrony Danych osobowych, znajdujących zastosowanie do danej czynności.

6.4. W przypadku uaktualnienia lub poszerzenia kategorii czynności przetwarzania Danych osobowych, IDS dokonuje niezwłocznego uaktualnienia Rejestru celem zapewnienia zgodności Rejestru ze stanem faktycznym oraz zakresem operacji przetwarzania Danych osobowych.

6.5. W miarę potrzeb w Rejestrze ujęte mogą być dodatkowe informacje zwiększające szczegółowość lub czytelność Rejestru jak również ułatwiające zarządzanie zgodnością ochrony Danych osobowych z wymogami prawa i realizację zasady rozliczalności.

6.6. IDS dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania poprzez wskazanie ogólnej podstawy prawnej przetwarzania, takiej jak np.: zgoda, umowa, obowiązek prawny nałożony na IDS.

§ 7 Realizacja obowiązków wobec osób, których dane osobowe dotyczą

7.1. IDS wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności, takich jak zgłoszenie sprzeciwu lub ograniczenie przetwarzania.

7.2. IDS dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których Dane osobowe przetwarza. IDS w regulaminach dostępnych w pokojach IDS publikuje informacje o zakresie przetwarzanych danych i prawach osób, których dane dotyczą i metodach kontaktu w zakresie danych osobowych;

7.3. W celu realizacji praw osoby, której Dane osobowe dotyczą IDS zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób, zintegrować te dane, wprowadzać w nich zmiany i usuwać w sposób zintegrowany.

7.4. IDS dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób, informując osobę, której dane dotyczą o:

- przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby,
- zmianie celu przetwarzania danych.
- uchyleniem ograniczenia przetwarzania.
- sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
- prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

7.5. IDS bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

7.6. Na żądanie osoby dotyczące dostępu do jej danych, IDS informuje, czy przetwarza dane osobowe, informuje o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela dostępu do danych. Dostęp do danych może być zrealizowany przez wydanie kopii danych lub przekazanie informacji określających zakres przetwarzanych danych.

7.7. IDS wydaje osobie, której Dane osobowe dotyczą, kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

7.8. IDS dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której Dane osobowe dotyczą. IDS ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych IDS informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.9. IDS uzupełnia i aktualizuje dane na żądanie osoby, której Dane osobowe dotyczą. IDS ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. IDS może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez IDS procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

7.10. Z uwzględnieniem ust. niżej, na żądanie osoby, IDS usuwa dane, gdy:

- dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
- zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
- osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
- dane były przetwarzane niezgodnie z prawem,
- konieczność usunięcia wynika z obowiązku prawnego.

7.11. IDS przy usuwaniu danych osobowych uwzględnia także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

7.12. Jeżeli dane podlegające usunięciu zostały przekazane przez IDS podmiotom trzecim, IDS podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych, IDS informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.13. IDS dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

- osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

- IDS nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
- osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie IDS zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

7.14. W trakcie ograniczenia przetwarzania IDS przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba, że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. IDS informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.15. Na żądanie osoby, IDS wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona IDS, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych IDS.

7.16. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, o którym mowa w art. 21 RODO, a dane przetwarzane są przez IDS na podstawie uzasadnionego interesu IDS lub powierzonego IDS zadania w interesie publicznym, IDS zobowiązuje się uwzględnić sprzeciw, o ile nie zachodzą po stronie IDS ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

7.17. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez IDS na potrzeby marketingu bezpośredniego, IDS uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

§ 8 Minimalizacja danych

8.1. IDS wdraża procedury służące realizacji zasady minimalizacji przetwarzanych Danych osobowych pod względem:

- adekwatności Danych osobowych do celów przetwarzania, obejmujących ograniczenie ilości przetwarzanych Danych osobowych oraz zakresu przetwarzania,
- ograniczenia dostępu do Danych osobowych wyłącznie do osób upoważnionych, dla których wykorzystanie Danych osobowych w określonym zakresie jest niezbędne dla prawidłowej realizacji obowiązków;
- ograniczenia czasu przechowywania Danych osobowych do okresu, dla którego przechowywanie Danych osobowych jest niezbędne ze względu na realizację celu przetwarzania lub obowiązków nałożonych na IDS.

8.2. IDS stosuje ograniczenia dostępu do Danych osobowych poprzez wdrożenie:

- zobowiązania Pracowników do zachowania poufności, w tym w zakresie Danych osobowych;
- weryfikacji wewnętrznych odbiorców Danych osobowych poprzez nadawanie poszczególnym Pracownikom szczegółowych upoważnień do przetwarzania Danych osobowych;

- środków technicznych ochrony Danych osobowych poprzez ograniczenie dostępu do systemów, oprogramowania oraz zasobów sieciowych wykorzystywanych w procesie przetwarzania Danych osobowych;
- fizycznych środków technicznych ochrony Danych osobowych, między innymi poprzez ograniczenie dostępu do pomieszczeń, w których odbywa się przechowywanie i przetwarzanie danych.

8.3. IDS dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.

8.4. IDS przetwarza dane osobowe z uwzględnieniem kryteriów wskazanych w Rejestrze i wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

8.5. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

§ 9 Bezpieczeństwo danych osobowych

9.1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia IDS wdraża środki techniczne i organizacyjne zapewniające należyty stopień ochrony Danych osobowych, odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.

9.2. IDS przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych i w tym celu kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia;

9.3. IDS wdraża środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

§ 10 Naruszenie ochrony danych osobowych

10.1. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:

- naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są Dane osobowe;
- udostępnienie Danych osobowych osobom nieupoważnionym;
- przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich przetwarzania;

- nieuprawnione lub przypadkowe uszkodzenie, utratę, zniszczenie lub zmianę Danych osobowych.

10.2. W przypadku stwierdzenia naruszenia ochrony danych osobowych, IDS dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych oraz szacuje skalę ryzyka i podejmuje stosowne działania.

10.3. W przypadku naruszenia ochrony Danych osobowych, IDS bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je właściwemu organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Wzór zawiadomienia, o którym mowa w zdaniu poprzedzającym, stanowi Załącznik nr 4 do Polityki.

10.4. Jeżeli ryzyko naruszenia praw i wolności osoby, której Dane osobowe dotyczą jest wysokie, IDS zawiadamia o incydencie także osobę, której danej dotyczą, chyba że:

- IDS wdroży odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- IDS zastosuje następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, lub wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

10.5. W przypadku stwierdzenia naruszenia ochrony danych osobowych, IDS dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych oraz szacuje skalę ryzyka. IDS dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w rejestrze naruszeń. Wzór rejestru naruszeń danych osobowych stanowi Załącznik nr 5 do Polityki.

§ 11 Powierzenie przetwarzania

11.1. IDS może powierzyć przetwarzanie Danych osobowych podmiotowi przetwarzającemu wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi w art. 28 ust. 3 RODO, powierzenie przetwarzania Danych osobowych, o którym mowa w zdaniu poprzedzającym, nie może prowadzić do naruszenia poufności danych.

11.2. IDS korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi i chroniło prawa osób, których dane dotyczą. W celu weryfikacji spełnienia obowiązku, o którym mowa w zdaniu poprzedzającym, IDS, przed powierzeniem przetwarzania potencjalnemu podmiotowi przetwarzającemu, w miarę możliwości uzyskuje informacje o zasadach ochrony Danych osobowych stosowanych przez potencjalny podmiot przetwarzający, oraz o praktykach tego podmiotu dotyczących zabezpieczenia Danych osobowych.

§ 12 Przekazywanie danych do Państwa trzeciego

12.1. IDS nie przekazuje Danych osobowych do państw trzecich położonych poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego, poza sytuacjami, w których następuje to na wniosek osoby, której Dane osobowe dotyczą.

12.2. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych, IDS okresowo weryfikuje zachowania użytkowników (w trakcie corocznego Audytu) oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

§ 13 Postanowienia końcowe

13.1. Polityka wchodzi w życie z dniem ogłoszenia.

13.2. W sprawach nieuregulowanych w Polityce odpowiednie zastosowanie znajdują postanowienia RODO, UODO oraz powszechnie obowiązujące przepisy prawa krajowego i europejskiego.

13.3. Wszelkie zmiany lub uzupełnienia do Polityki wymagają dla swej skuteczności formy pisemnej pod rygorem nieważności. Zmiany lub uzupełnienia do Polityki wchodzą w życie nie wcześniej niż w terminie 7 dni od dnia ich ogłoszenia.

13.4. Do Polityki dołączono następujące Załączniki, stanowiące integralną część Polityki:

- Załącznik nr 1 – Lista zbiorów danych w IDS,
- Załącznik nr 2 – Wzór upoważnienia do przetwarzania danych osobowych i jego odwołania;
- Załącznik nr 3 – Rejestr czynności przetwarzania;
- Załącznik nr 4 – Wzór zgłoszenia naruszenia ochrony danych osobowych;
- Załącznik nr 5 – Rejestr naruszeń danych osobowych.

Załącznik nr 1 – Lista Zbiorów danych w IDS

Uwzględniając definicję z art. 4 pkt 6 RODO IDS przetwarzana Dane osobowe zgrupowane w następujących Zbiorach danych:

1. **Pracownicy IDS** – obejmujący dane osobowe osób fizycznych zatrudnionych w IDS na podstawie stosunku pracy (niezależnie od podstawy jego nawiązania), dane osobowe osób fizycznych współpracujących z IDS na podstawie umowy cywilnoprawnej (umowy zlecenie, umowy o dzieło) oraz dane osobowe praktykantów i stażystów IDS;
2. **Klienci** – obejmujący dane osobowe klientów będących osobami fizycznymi, w tym prowadzącymi jednoosobową działalność gospodarczą, jak również dane osobowe osób fizycznych będących przedstawicielami (reprezentantami) klientów (członkowie zarządów, prokurenci i pełnomocnicy osób prawnych; pracownicy klientów występujący w imieniu kontrahentów);
3. **Dostawcy** – obejmujący dane osobowe dostawców będących osobami fizycznymi prowadzącymi jednoosobową działalność gospodarczą, jak również dane osobowe osób fizycznych będących przedstawicielami (reprezentantami) dostawców (członkowie zarządów, prokurenci i pełnomocnicy osób prawnych; pracownicy dostawców występujący w imieniu kontrahentów);
4. **Pracownicy kontrahentów** – obejmujące dane osobowe pracowników oraz współpracowników firm świadczących usługi na rzecz IDS,
5. **Przedstawiciele organów** – obejmujący dane osobowe przedstawicieli organów administracji publicznej oraz innych instytucji publicznych;
6. **Dane nieidentyfikowane** – Dane osobowe nieidentyfikowane przez IDS, takie jak dane osób monitorowanych przy wykorzystaniu systemu monitoringu wizyjnego;

miejscowość, data

UPOWAŻNIENIE Nr_____
DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem ..... r., upoważniam Pana/Panią ..... do przetwarzania danych osobowych powierzonych przez Instytut Doskonałości Strategicznej Sp. z o.o. w ramach Umowy z dnia .....r.

Upoważnienie wygasa z chwilą ustania Pana/Pani* zatrudnienia/współpracy w Instytucie Doskonałości Strategicznej/wykonywania zadań na podstawie stosunku cywilnoprawnego*, lub z chwilą jego odwołania.

_____

czytelny podpis osoby upoważnionej
do wydawania i odwoływania upoważnień

Upoważnienie otrzymałem:

Toruń, ... r., _____
(miejscowość, data, podpis osoby upoważnionej)

Oświadczam, że zapoznałem/am* się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, z późn. zm.), a także z obowiązującymi w Instytucie Doskonałości Strategicznej Sp. z o.o. Polityką przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie trwania umowy jak również po ustania stosunku prawnego łączącego mnie z Instytutem Doskonałości Strategicznej Sp. z o.o..

_____
czytelny podpis osoby składającej oświadczenie

*niepotrzebne skreślić

miejscowość, data

ODWOŁANIE UPOWAŻNIENIA Nr _____
DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem .....r., odwołuję upoważnienie Pana/Pani* ..... do przetwarzania danych osobowych nr ..... wydane w dniu ..... r.

_____

czytelny podpis osoby upoważnionej
do wydawania i odwoływania upoważnień

..... r.
(miejscowość, data)

*niepotrzebne skreślić

Załącznik nr 3 – Rejestr czynności przetwarzania

Rejestr czynności przetwarzania
IDS

Administrator Danych: IDS

Czynność przetwarzania	Cel przetwarzania	Podstawa przetwarzania	Kategorie osób	Kategorie danych	Kategorie odbiorców	Sposób przetwarzania danych	Okres przechowywania danych	Stosowane środki bezpieczeństwa
Obsługa stosunku pracy i współpracy	Zarządzanie personelem, realizacja uprawnień i obowiązków pracodawcy wynikających z Kodeksu pracy	W zakresie danych, o których mowa w art. [•] Kodeksu Pracy: Umowa o pracę z dnia [•] (art. 6 ust. 1 lit. b). W pozostałym zakresie – zgoda pracownika z dnia [•]	Pracownicy Kancelarii zatrudnieni w kancelarii na podstawie stosunku pracy	Imię, nazwisko, data urodzenia, PESEL, numer telefonu pracownika, mail służbowy i prywatny, miejsce zamieszkania	Zarząd/Właściciel Kancelarii, inne spółki z grupy kapitałowej, pracownicy/podmiot świadczący obsługę kadrowo-płacową kancelarii, dostawca powierzchni dyskowej w chmurze	papierowo oraz elektronicznie	Czas trwania stosunku pracy oraz okres archiwizacji i przechowywania dokumentów pracowniczych wymagany przepisami prawa	
Obsługa klientów				Imię, nazwisko, data urodzenia, PESEL, numer telefonu mail, miejsce zamieszkania				

Załącznik nr 4 – Wzór zgłoszenia naruszenia ochrony danych osobowych

Toruń, dnia ……

Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

Zgłoszenie naruszenia ochrony danych osobowych

Działając w imieniu IDS z siedzibą przy ul. Gagarina 5/102, 87-100 Toruń, na podstawie przyznanego mi uprawnienia oraz na podstawie art. 33 ust. 1 i 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych i Ustawy o Ochronie Danych Osobowych z 10 maja 2018 r., niniejszym zgłaszam następujące naruszenie ochrony danych osobowych:

Administrator Danych Osobowych oraz dane kontaktowe naruszenia:	Instytut Doskonałości Strategicznej Sp. z o.o., ul. Jurija Gagarina 5/105, 87-100 Toruń, NIP 9562319177
Data zaistnienia naruszenia:	
Kategorie i przybliżoną liczbę osób, których dane dotyczą:	
Kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie:	
Opisać możliwe konsekwencje naruszenia ochrony danych osobowych:	
Opisać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych:	

_____

Podpis

Załącznik nr 5 – Rejestr naruszeń danych osobowych w IDS

Lp.	Opis naruszenia	Data zajścia naruszenia	Kategoria i ilość osób, których dotyczy naruszenie	Zakres danych i/lub kategorie danych, których dotyczy naruszenie	Okoliczności naruszenia - opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia	Opis skutków /konsekwencji naruszenia	Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowane środki zastosowane w celu zminimalizowania jego negatywnych skutków	Rezultat działań naprawczych