

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH



Krzysztof Pakulski - PPHU ALLTERM -

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

SPIS TREŚCI

Wstęp	2
1. Postanowienia ogólne	3
2. Definicje	5
3. Obowiązek informacyjny o przetwarzaniu danych	7
4. Wykaz zbiorów danych osobowych	7
5. Zakres stosowania.....	9
6. Obowiązki i odpowiedzialność administratora danych osobowych.	10
7. Zarządzanie ochroną danych osobowych	12
8. Upoważnienie do przetwarzania danych osobowych	12
9. Obowiązki osób upoważnionych do przetwarzani danych osobowych	13
10. Ewidencja osób upoważnionych	14
11. Szkolenia pracowników	14
12. Udostępnianie danych osobowych	15
13. Programy komputerowe użytkowane do przetwarzania danych osobowych	15
14. Powierzenie do przetwarzania	16
15. Bezpieczeństwo usług zewnętrznych	16
16. Środki organizacyjne i techniczne bezpieczeństwa przetwarzania danych	17
17. Ochrona danych osobowych w korespondencji elektronicznej	18
18. Niszczenie dokumentacji papierowej i na nośnikach elektronicznych.	19
19. Postępowanie w przypadku naruszenia ochrony danych osobowych	20
20. Zgodność polityki bezpieczeństwa danych z aktualnym stanem prawnym	22
21. Postanowienia końcowe	22

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w całości lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

Wstęp. Polityka bezpieczeństwa danych osobowych

Procedura Polityki Bezpieczeństwa Danych Osobowych zawarta w niniejszym dokumencie została opracowana w oparciu o wymagania zawarte w Rozporządzeniu Parlamentu Europejskiego i Rady (dalej RODO) /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 /Dz. Urz. UE. L nr 119, str.1/, Dokument zawiera sposób przygotowania i zbiór dokumentacji opisującej politykę bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony określonych w rozporządzeniu.

Rozporządzenie RODO wiąże w całości, jest stosowane bezpośrednio i nie wymaga przystosowania do porządków krajowych poszczególnych państw, dlatego jest instrumentem pozwalającym na silniejsze zbliżenie prawa, kompleksowo regulując ochronę danych osobowych w Unii Europejskiej.

Kreując politykę bezpieczeństwa przetwarzania danych, RODO zakłada indywidualne podejście w tej kwestii każdego przedsiębiorstwa w celu wdrożenia niezbędnych zabezpieczeń, które spełnią wymogi RODO i będą skutecznie chronić prawa osób. W tym celu konieczne jest uwzględnienie poziomu wiedzy na temat zabezpieczeń technicznych, zakresu i celów przetwarzania, ryzyka naruszenia praw lub wolności osób fizycznych wynikających z przetwarzania. Administrator Danych Osobowych (dalej: Administrator) na podstawie zebranych danych, odpowiedzialny jest za wdrożenie odpowiednich środków technicznych i organizacyjnych, zarówno przy określeniu sposobów przetwarzania, jak i w czasie samego przetwarzania.

Istotne jest też budowanie świadomości pracowników, postępowanie zgodnie z przyjętymi zasadami, raportowanie zagrożeń i incydentów, regularny udział w szkoleniach z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji oraz reagowanie na zmieniające się otoczenie wewnętrzne i zewnętrzne w firmie.

W celu ochrony danych osobowych Administratorzy danych (firmy, organizacje itp.) powinni zorganizować odpowiednią strukturę oraz wdrożyć zabezpieczenia techniczne i organizacyjne dla skutecznego zarządzania bezpieczeństwem danych osobowych.

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakiegokolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

O tych właśnie zagadnieniach mówi Polityka bezpieczeństwa przetwarzania danych osobowych.

1. Postanowienia ogólne

- 1.1. Artykuł 24 RODO zobowiązuje Administratora do wdrożenia odpowiednich środków technicznych i organizacyjnych realizujących wytyczne RODO poprzez wdrażaniu środków gwarantujących organizacyjne i techniczne bezpieczeństwo przetwarzania danych osobowych
- 1.2. Celem Polityki Bezpieczeństwa Przetwarzania Danych Osobowych, zwanej dalej „Polityką bezpieczeństwa” w Krzysztof Pakulski - PPHU ALLTERM -, zwanej dalej „Administratorem”, jest zapewnienie ochrony danych osobowych przetwarzanych przez Administratora przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.
- 1.3. Celem Polityki Bezpieczeństwa jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczać dane osobowe. Podstawowe z tych działań to organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych osobowych oraz edukowanie użytkowników systemu ochrony danych osobowych.
- 1.4. Polityka Bezpieczeństwa dotyczy zadań związanych z zabezpieczeniem danych osobowych zarówno przetwarzanych w sposób tradycyjny (wersje papierowe) jak i w systemach informatycznych. Osoby mające kontakt z zbiorami zawierającymi dane osobowe zobowiązane są do przestrzegania postanowień Polityki Bezpieczeństwa.
- 1.5. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady postępowania przy przetwarzaniu danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.
- 1.6. Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie bezpieczeństwa danych osobowych, przetwarzanych przez Krzysztof Pakulski - PPHU

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

ALLTERM - rozumianej jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

- 1.7. Polityka Bezpieczeństwa przetwarzania danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.
- 1.8. Administratorem przetwarzanych danych osobowych jest Krzysztof Pakulski - PPHU ALLTERM -.
- 1.9. Administrator powołał/ nie powołał/* inspektora ochrony danych, zgodnie art. 37 RODO. Wzór dokumentu powołania stanowi Załącznik Nr 1.
- 1.10. Dopuszcza się powołanie jednego wspólnego inspektora ochrony danych dla grupy przedsiębiorstw pod warunkiem spełnienia warunków określonych w art. 37 RODO. Zadania inspektora ochrony danych zawarte są w art. 39 RODO.
- 1.11. Obszarem przetwarzania danych osobowych przez Krzysztof Pakulski - PPHU ALLTERM - jest każdorazowy adres siedziby Administratora.
- 1.12. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Krzysztof Pakulski - PPHU ALLTERM - rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa przetwarzanych danych osobowych jest akceptowalna wielkość ryzyka związanego z ochroną przetwarzanych danych.
- 1.13. Zastosowane zabezpieczenia jakie podejmuje Administrator mają służyć osiągnięciu bezpieczeństwa przetwarzanych danych i zapewnić:
 - 1.13.1. poufność danych – polega na zapewnieniu, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.
 - 1.13.2. integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

- 1.13.3. rozliczalność danych – oznaczająca, że działania osób mogą być przypisane w sposób jednoznaczny tylko tym osobom,
- 1.13.4. autentyczność – polegająca na zapewnieniu, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
- 1.13.5. integralność systemu – co oznacza, niemożność jakiegokolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej przy systemach operacyjnych,
- 1.13.6. dostępność informacji – zapewnienie osoby upoważnionym dostępu do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
- 1.13.7. braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
- 1.13.8. zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

2. Definicje

2.1. Przez użyte w Polityce Bezpieczeństwa określenia zgodnie z art. 4 RODO należy rozumieć:

- 2.1.1. **administrator danych osobowych** – zgodnie z art. 4 ust. 7 RODO, jest to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
- 2.1.2. **inspektor ochrony danych** – zgodnie z art. 37 ust. 1 RODO, jest to osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,
- 2.1.3. **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

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w całości lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str. 1/,

- 2.1.4. dane osobowe** – zgodnie z art. 4 ust. 1 RODO, są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
- 2.1.5. zbiór danych osobowych** – zgodnie z art. 4 ust. 6 RODO, jest to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
- 2.1.6. przetwarzane danych** – zgodnie z art. 4 ust. 2, są to operacje lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.
- 2.1.7. system informatyczny** – jest **zestaw** urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, współpracujących ze sobą w celu przetwarzania danych osobowych,
- 2.1.8. system tradycyjny** – to wyposażenie i środki trwale wykorzystywane w celu przetwarzania danych osobowych na papierze,
- 2.1.9. zabezpieczenie danych w systemie informatycznym** – to zapewnienie poprzez wdrożenie procedur i środków technicznych ochrony danych przed ich nieuprawnionym przetwarzaniem
- 2.1.10. administrator systemu informatycznego** – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,
- 2.1.11. podmiot przetwarzający** - zgodnie z art. 4 ust. 8 RODO osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, upoważniona przez administratora do przetwarzania danych w jego imieniu,
- 2.1.12. odbiorca** – zgodnie z art. 4 ust. 9 RODO to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

- 2.1.13. **strona trzecia** – zgodnie z art. 4 ust. 10 RODO to osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,
- 2.1.14. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
- 2.1.15. **zgoda osoby** – zgodnie z art. 4 ust. 11 RODO to świadome i dobrowolne okazanie woli,
- 2.1.16. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

3. Obowiązek informacyjny.

- 3.1. Zgodnie z art. 13 RODO w przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych Ustawą należy poinformować tę osobę o:
 - 3.1.1. Pełnej nazwie Administratora i adresie siedziby,
 - 3.1.2. Celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
 - 3.1.3. Prawie dostępu do swoich danych oraz ich poprawiania,
 - 3.1.4. Dobrowolności lub obowiązku podania danych - jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
 - 3.1.5. Wzór Klauzuli Informacyjnej stanowi Załącznik Nr 2

4. Wykaz zbiorów danych osobowych

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakiegokolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

- 4.1.** Zbiór danych osobowych to zbiór spełniający przesłanki: zawiera dane osobowe, ma określoną, własną strukturę oraz zapewnia dostęp do danych według określonych kryteriów. Za zbiór danych można uznać wszelkie materiały gromadzone w formie akt.
- 4.2.** Dane osobowe gromadzone są w zbiorach :
- 4.2.1.** Ewidencja osób upoważnionych do przetwarzania danych osobowych,
 - 4.2.2.** Akta osobowe pracowników – przykładowa struktura zbioru
 - 4.2.2.1. Imię, nazwisko,
 - 4.2.2.2. płeć,
 - 4.2.2.3. pesel,
 - 4.2.2.4. seria i numer dowodu,
 - 4.2.2.5. Adres do korespondencji,
 - 4.2.2.6. urząd skarbowy,
 - 4.2.2.7. data urodzenia
 - 4.2.3.** Zbiory informacji o pracownikach, oświadczenia na potrzeby ZFŚS,
 - 4.2.4.** Ewidencja zwolnień lekarskich,
 - 4.2.5.** Skierowania na badania okresowe, specjalistyczne,
 - 4.2.6.** Ewidencja urlopów, czasu pracy, wyjść,
 - 4.2.7.** Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej,
 - 4.2.8.** Rejestr delegacji służbowych,
 - 4.2.9.** Listy płac pracowników,
 - 4.2.10.** Deklaracje ubezpieczeniowe pracowników,
 - 4.2.11.** Deklaracje i kartoteki ZUS pracowników,
 - 4.2.12.** Deklaracje podatkowe pracowników,
 - 4.2.13.** Rejestr wypadków,
 - 4.2.14.** Umowy cywilno-prawne,
 - 4.2.15.** Umowy zawierane z kontrahentami,
 - 4.2.16.** Rejestr klientów,
 - 4.2.17.** Dokumenty archiwalne,

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

5. Zakres stosowania

- 5.1.** Krzysztof Pakulski - PPHU ALLTERM - jako Administrator przetwarza dane osobowe: pracowników, byłych pracowników, stażystów, klientów, kontrahentów, odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia Administratora oraz osób współpracujących na podstawie umów cywilnoprawnych, w tym danych osobowych i treści zawieranych umów.
- 5.2.** Do przetwarzania danych administrator używa postaci dokumentacji tradycyjnej (papierowej) i w formie elektronicznej.
- 5.3.** Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
- 5.4.** Krzysztof Pakulski - PPHU ALLTERM - jako Administrator reguluje również ochronę danych osobowych za pomocą dodatkowych dokumentów jakimi są:
- 5.4.1.** ewidencja osób upoważnionych do przetwarzania danych osobowych Załącznik Nr 4,
 - 5.4.2.** rejestr naruszeń Załącznik Nr 9,
 - 5.4.3.** rejestr czynności przetwarzania danych osobowych Załącznik Nr 8,
 - 5.4.4.** procedura postępowania w przypadku naruszenia ochrony danych osobowych.
- 5.5.** Polityka Bezpieczeństwa dotyczy również wszystkich Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych oraz osób dopuszczonych do przetwarzania danych osobowych.
- 5.6.** Polityka bezpieczeństwa określona jest również przez zasady bezpieczeństwa obowiązujące użytkowników przetwarzających dane osobowe, z którymi należy zapoznać użytkowników komputerów na których przetwarzane są te. Zbiór zasad stanowi Załącznik Nr 6.
- 5.7.** Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

- 5.7.1. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz dokumentów papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
- 5.7.2. wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
- 5.7.3. wszystkich pracowników, byłych pracowników, przyszłych pracowników, stażystów, i innych osób mających dostęp do informacji podlegających ochronie

6. Obowiązki i odpowiedzialność Administratora

6.1. Do najważniejszych obowiązków Administratora należy:

- 6.1.1. Przetwarzanie danych osobowych wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z warunków określonych w art. 6 RODO,
- 6.1.2. Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych oraz innych przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych,
- 6.1.3. Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa,
- 6.1.4. Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
- 6.1.5. Przeprowadzanie szkoleń użytkowników przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe,
- 6.1.6. Prowadzenie ewidencji czynności przetworzenia danych osobowych,
- 6.1.7. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
- 6.1.8. Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
- 6.1.9. Nadzór nad bezpieczeństwem danych osobowych,
- 6.1.10. Kontrola działań pracowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w całości lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakiegokolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

- 6.1.11. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
 - 6.1.12. Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
 - 6.1.13. Optymalizacja wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
 - 6.1.14. Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
 - 6.1.15. Konfiguracja i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
 - 6.1.16. Współpraca z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
 - 6.1.17. Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
 - 6.1.18. Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
 - 6.1.19. Zmiana lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
 - 6.1.20. Zarządzanie licencjami oraz procedurami ich dotyczącymi,
 - 6.1.21. Prowadzenie profilaktyki antywirusowej.
- 6.2. Część zadań zakresu objętego ust. 1 ppkt 6.1.11 do 6.1.20 w przypadku braku w własnych działów informatycznych Administrator może powierzyć na podstawie umowy wraz z upoważnieniem do przetwarzania części danych osobowych, firmom informatycznym świadczącym obsługę informatyczną dla Administratora.

7. Zarządzanie ochroną danych osobowych.

7.1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.

- 7.2. dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.
- 7.3. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.
- 7.4. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.
- 7.5. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.
- 7.6. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
- 7.7. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

8. Upoważnienie do przetwarzania danych osobowych

- 8.1. Administrator jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, czyli jednym z najważniejszych obowiązków administratora danych jest posiadanie wiedzy nad tym kto, kiedy i w jakim zakresie ma dostęp do jego zasobów chronionych.
- 8.2. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora na mocy art. 28 RODO (Załącznik Nr 3).
- 8.3. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora.
- 8.4. W celu otrzymania przez Użytkownika upoważnienia do przetwarzania danych osobowych, należy dostarczyć do Administratora podpisane oświadczenie użytkownika.
- 8.5. Na podstawie otrzymanego oświadczenia Administrator upoważnia Użytkownika

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w całości lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

do przetwarzania danych osobowych i wydaje upoważnienie do przetwarzania danych osobowych. Upoważnienia, o których mowa powyżej przechowywane przez Administratora.

- 8.6.** Upoważnienie może być w każdym czasie odwołane przez Administratora. Oświadczenie o odwołaniu upoważnienia do przetwarzania danych osobowych powinno być sporządzone na piśmie. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą ustania przesłanki będącej podstawą wydania upoważnienia, w tym w szczególności wygaśnięcia stosunku pracy lub umowy cywilnoprawnej łączącej Użytkownika z Administratorem.

9. Obowiązki osób upoważnionych do przetwarzania danych osobowych

9.1. Do najważniejszych obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

- 9.1.1.** Znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom, nieuprawnionym dostępu do swojej stacji roboczej,
- 9.1.2.** Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami,
- 9.1.3.** Prowadzenie rejestru czynności przetwarzania na zasadach określonych w art. 30 RODO. Wzór rejestru stanowi Załącznik Nr 8.
- 9.1.4.** Postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych,
- 9.1.5.** Zachowania w tajemnicy danych osobowych, do których uzyskały dostęp oraz informacji o sposobach ich zabezpieczenia,
- 9.1.6.** Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

- 9.1.7. Informowania Administratora o wszelkich podejrzaniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe,
- 9.1.8. Zapoznanie się z Polityką Bezpieczeństwa przetwarzania danych osobowych oraz o ile funkcjonuje Instrukcją Zarządzania Systemem Informatycznym, służącym do przetwarzania danych osobowych.

10. Ewidencja osób upoważnionych.

- 10.1. Zgodnie z art. 39 RODO Administrator prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
- 10.2. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora zgodnie ze wzorem formularza stanowiącym Załącznik nr 4 do Polityki Bezpieczeństwa przetwarzania danych osobowych.

11. Szkolenia użytkowników

- 11.1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
- 11.2. Za przeprowadzenie szkolenia odpowiada Administrator.
- 11.3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami RODO, Polityką Bezpieczeństwa danych i Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych obowiązującymi u Administratora.

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

Po zaznajomieniu się z powyższymi regulacjami, użytkownik, przed dopuszczeniem do przetwarzania danych, powinien zobowiązać się do ich przestrzegania przez podpisanie oświadczenia użytkownika, stanowiącego Załącznik nr 3.

12. Udostępnianie danych osobowych.

- 12.1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą,
- 12.2. Zgodnie z RODO udostępnienie danych może nastąpić:
 - 12.2.1. z uwzględnieniem przepisów prawa,
 - 12.2.2. w sytuacjach, gdy jest ono niezbędne do realizacji prawnie uzasadnionych celów administratora,
 - 12.2.3. za wyraźną zgodą podmiotu, którego dane dotyczą.
- 12.3. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora.
- 12.4. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
- 12.5. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

13. Programy informatyczne wykorzystywane do przetwarzania danych.

- 13.1. Do przetwarzania danych osobowych w Krzysztof Pakulski - PPHU ALLTERM - wykorzystywane są programy informatyczne wg Załącznika Nr 11.
- 13.2. Programy te posiadają licencje na użytkowanie i są aktualizowane zgodnie z informacją od dostawców.
- 13.3. Programy umieszczone są na serwerze w pomieszczeniu zamkniętym i chronionym.

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

13.4. Dostęp do serwera z komputerów użytkowników odbywa się za pomocą sieci zabezpieczonej przed nieuprawnionym dostępem.

14. Powierzenie do przetwarzania.

14.1. Administrator może powierzyć dane osobowe do przetworzenia zewnętrznym firmom świadczącym wyspecjalizowane usługi kadrowe, księgowość czy też informatyczne. Zawarcie Umowy powierzenia wymaga formy pisemnej. Wzór Załącznik Nr 7.

14.2. Zgodnie z art. 28 ust. 1 RODO Administrator powinien korzystać wyłącznie z usług podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

14.3. Umowa powierzenia (Załącznik Nr 7) powinna zawierać następujące elementy

- 14.3.1. przedmiot przetwarzania,
- 14.3.2. czas trwania przetwarzania,
- 14.3.3. charakter i cel przetwarzania,
- 14.3.4. rodzaj danych osobowych,
- 14.3.5. kategorię osób, których dane dotyczą,
- 14.3.6. obowiązki i prawa administratora,
- 14.3.7. obowiązki podmiotu przetwarzającego.

15. Bezpieczeństwo usług zewnętrznych.

14.1. Należy zapewnić aby usługi zewnętrzne były prowadzone wyłącznie zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych obowiązującymi w Krzysztof Pakulski - PPHU ALLTERM -, wymaganiami umowy oraz wymaganiami prawa.

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w całości lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakiegokolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

- 14.2. Wymagania bezpieczeństwa przetwarzania danych osobowych, zakres usług oraz poziom ich dostarczania należy określić w umowie świadczenia usług.
- 14.3. Należy zapewnić aby użytkownicy nie będący pracownikami NAZWA FIRMY stosowali te same zasady bezpieczeństwa przetwarzania danych osobowych co użytkownicy będący pracownikami.

16. Środki organizacyjne i techniczne zabezpieczenia przetwarzania danych osobowych.

- 16.1. Dane osobowe mogą być przetwarzane wyłącznie w obszarze przetwarzania danych osobowych, na które składają się pomieszczenia biurowe w siedzibie Administratora, z wyjątkiem sytuacji udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych. Szczegółowy wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych znajduje się w Załączniku nr 10 do Polityki Bezpieczeństwa.
- 16.2. Dane osobowe Administrator przetwarza przy zastosowaniu zabezpieczeń zapewniających ich ochronę w postaci środków organizacyjnych, technicznych i środków ochrony fizycznej.
- 16.3. Dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych stosuje się następujące środki:
 - 16.3.1. Środki organizacyjne:
 - wdrożenie Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych,
 - ustalona, indywidualna procedura udzielania upoważnień przez Administratora poprzedzonego szkoleniem z zakresu przepisów i zasad ochrony danych osobowych,
 - prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych, procedura postępowania w sytuacji naruszenia ochrony danych osobowych, konieczność składania deklaracji poufności przez Użytkowników danych, procedury przechowywania zbiorów danych.

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w całości lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

16.3.2. Środki techniczne:

- zbiory danych osobowych przetwarzane są wyłącznie na autoryzowanym sprzęcie służbowym,
- stacje robocze wyposażone są w indywidualną ochronę antywirusową;
- dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

16.3.3. Środki ochrony fizycznej:

- pomieszczenia, w których znajdują się zbiory danych osobowych, są zamykane na klucz, a dostęp do nich odbywa się wyłącznie w obecności pracowników Administratora,
- pomieszczenia, w którym przetwarzany jest zbiór danych osobowych znajdują się wewnątrz budynku w strefie ograniczonego dostępu,
- zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie,
- dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek.

17. Ochrona danych osobowych w korespondencji elektronicznej

17.1. Korespondencja, która zawiera dane osobowe, powinna być przesyłana w formie zaszyfrowanego pliku, natomiast hasło przekazywać innym kanałem komunikacyjnym. Praktyka ta ma zapobiec sytuacji, w której wysyłamy dane osobowe w treści wiadomości e-mail i podczas wyboru adresata mylimy się, co skutkuje wysłaniem wiadomości do osoby nieuprawnionej do jej otrzymania.

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w całości lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

- 17.2. Mechanizmem, który może uchronić użytkownika przed mylnym wyborem adresata jest wyłączenie funkcji podpowiadania adresu e-mail – oczywiście jest to pewnego rodzaju utrudnienie, ponieważ przy adresowaniu każdej wiadomości musimy wprowadzić cały adres e-mail, jednak mechanizm ten bardzo często uchroni nas przed wyborem nieodpowiedniego adresata.
- 17.3. Wysyłka korespondencji masowej do wielu adresatów wymaga ukrycia adresów odbiorców. Jeżeli tego nie zrobimy wszyscy odbiorcy będą widzieli adresy e-mail pozostałych osób. Taka sytuacja doprowadza do masowego upublicznienia danych osobowych. W przypadku wysyłania korespondencji masowej np. newsletter należy skorzystać z opcji „UDW” (kopia ukryta), która zapobiegnie wystąpieniu incydentu.

18. Niszczenie dokumentacji papierowej i w formie zapisu elektronicznego na dysku komputerów i urządzeń przenośnych.

- 18.1. Zgodnie art. 5 lit e dane osobowe powinny być przechowywane przez okres nie dłuższy niż jest to niezbędne do celów, w których dane są przetwarzane.
- 18.2. RODO zastrzega przepisy dotyczące niszczenia dokumentów.
- 18.3. Dokumenty zawierające dane osobowe w formie papierowej mają być niszczone w niszczarkach mechanicznych posiadających urządzenia tnące uniemożliwiające odczyt zniszczonych dokumentów lub mogą przekazywane do niszczenia firmom zewnętrznym gwarantującym ochronę przekazanych danych osobowych i profesjonalizm.
- 18.4. Dane na komputerach i urządzeniach przenośnych typu laptopy, smartfony, mają być usuwane z pamięci dysków. Za pomocą przebijaka do dysku twardego można zniszczyć niepotrzebne dane elektroniczne bezpiecznie, wygodnie i niezawodnie.
- 18.5. Chcąc zminimalizować ryzyko utraty danych z pamięci USB zaleca się dopuszczanie do użytkowania przez pracowników jedynie firmowych pamięci USB, które są zaszyfrowane.

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakiegokolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

19. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych.

- 19.1.** Każdy użytkownik w przypadku stwierdzenia lub podejrzenia stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym poinformować Administratora Danych.
- 19.2.** Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
- 19.2.1.** Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
 - 19.2.2.** Niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekami, kradzieżami i utratą danych osobowych;
 - 19.2.3.** Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.
- 19.3.** Do typowych incydentów bezpieczeństwa danych osobowych należą:
- 19.3.1.** Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
 - 19.3.2.** Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twarde dyski, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych);
 - 19.3.3.** Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
- 19.4.** W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych uruchamia Procedurę i prowadzi postępowanie wyjaśniające w toku którego:
- 19.4.1.** Ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
 - 19.4.2.** Inicjuje ewentualne działania dyscyplinarne,
 - 19.4.3.** Rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w całości lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakiegokolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

19.4.4. Dokumentuje prowadzone postępowania.

19.5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:

19.5.1. Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,

19.5.2. Zabezpiecza ewentualne dowody;

19.5.3. Ustala osoby odpowiedzialne za naruszenie;

19.5.4. Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);

19.5.5. Inicjuje działania dyscyplinarne;

19.5.6. Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;

19.5.7. Dokumentuje prowadzone postępowania zgodnie ze wzorem Raportu z naruszenia bezpieczeństwa danych osobowych stanowiących Załącznik nr 9 do Polityki Bezpieczeństwa.

20. Zgodność polityki bezpieczeństwa przetwarzania danych z aktualnym stanem prawnym.

20.1. Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Krzysztof Pakulski - PPHU ALLTERM -, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

20.2. Administrator raz w roku sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

20.3. Okresowy przegląd Polityki Bezpieczeństwa powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Administratora oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w całości lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Polityka bezpieczeństwa przetwarzania danych osobowych

W Krzysztof Pakulski - PPHU ALLTERM -

21. Postanowienia końcowe.

- 21.1. Administrator ma obowiązek zapoznać z treścią Polityki Bezpieczeństwa każdego użytkownika przetwarzającego dane osobowe.
- 21.2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiegokolwiek innej formie.
- 21.3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
- 21.4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
- 21.5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
- 21.6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.

Dokumentacja, dotycząca ochrony danych osobowych, pozyskana ze strony internetowej spółki **2S1 Sp. z o.o.**, podlega ochronie prawnej na podstawie ustawy z dnia 04.02.1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2017, poz. 880 z późn. zm.). Żaden dokument w części lub każdy z osobna w całości, nie może być powielany, ani rozpowszechniany w jakiegokolwiek formie i w jakikolwiek sposób na jakichkolwiek polach eksploatacji, włącznie z kopiowaniem, fotokopiowaniem, przedrukowywaniem i digitalizacją, w tym także zamieszczaniem w Internecie, bez pisemnej zgody spółki **2S1 Sp. z o.o.** Jakiegokolwiek użycie lub wykorzystanie przedmiotowej dokumentacji w całości lub w części w innych celach niż niekomercyjne cele prywatne, bez zgody spółki **2S1 Sp. z o.o.**, stanowi naruszenie przepisów prawa.

Dokumenty nr TR/BSG/295/28/6

Zarządzenie w sprawie powołania inspektora ochrony danych

W

Zarządzenie nr ...

z 2018 r.

w sprawie powołania wspólnego inspektora ochrony danych

Na podstawie art. 37 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady/UE z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zarządza się co następuje:

Powołuje się Pana/Panią, pracownika, na inspektora ochrony/wspólnego inspektora danych */ w

Zakres działania inspektora / wspólnego inspektora/* ochrony danych obejmuje następujące jednostki organizacyjne:

.....

W załączniku do niniejszego zarządzenia ustala się ramowy zakres zadań wspólnego/ inspektora/* ochrony danych.

Traci moc zarządzenie nr z w sprawie powołania administratora bezpieczeństwa informacji w */

Zarządzenie wchodzi w życie 2018 r.

Uwaga: / niepotrzebne skreśl*

KLAUZULA INFORMACYJNA w
ochrony danych osobowych

Zgodnie z art. 13 ust. 1-2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku 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.U.UE.L.2016.119.1) – dalej RODO informujemy, że:

1. Administrator Danych Osobowych :

Administratorem Pani/Pana danych osobowych jest
z/szarejestrowana w Krajowym Rejestrze Sądowym prowadzonym przez Sąd Rejonowy w pod numerem, NIP: REGON.....

2. Inspektor Ochrony Danych Osobowych / Pełnomocnik ds. osobowych*

.....
Jest organem Administratora, z którym Pan/Pani może się kontaktować tel. [...], pod e-mailem [...] lub pisemnie na adres siedziby wskazany w pkt. 1

3. Cele i podstawy przetwarzania.

3.1. Pani/Pana dane osobowe przetwarzane będą w celu przeprowadzenia rekrutacji na stanowisko pracy na jakie złożył Pan/Pani na podstawie art. 6 ust 1b lub/i na podstawie art. 6 ust 1 pkt a RODO w celu przetwarzania danych kontaktowych lub/i przyszłych rekrutacji na podstawie zgody na przetwarzanie w określonym w zgodzie celu.

TAK * NIE *

3.2. Jako Administrator będziemy przetwarzać Pana/Pani dane osobowe, określone w art. 4 ust. 1 RODO, zgodnie z udzielonym upoważnieniem w celu:

3.2.1.1 zawarcia umowy [...] na podstawie Pana/Pani zainteresowania naszą ofertą (art 6 ust. 1 lit. b RODO)

TAK * NIE *

3.2.1.2 wykonania umowy, gdy ją zawarliśmy (podstawa z art. 6 ust. 1 lit. b RODO)

TAK * NIE *

3.3. w celu ewentualnego ustalenia, dochodzenia lub obrony przed roszczeniami będącego naszego prawnie uzasadnionego w tym interesu (podstawa art.6 ust. 1 lit. f RODO).

3.4. w celach archiwalnych (dowodowych) będących realizacją naszego interesu zabezpieczenia informacji na wypadek prawnej potrzeby wykazania faktów (podstawa art.6 ust. 1 lit. f RODO) przez okres wskazany w przepisach prawa.

3.5. w celu wypełnienia obowiązku prawnego ciążącego na administratorze w zakresie informacji skarbowych, sądowych itp.

4. Prawo do odwołania zgody na przetwarzanie danych.

4.1. W każdym czasie przysługuje Pan/Pani prawo do odwołania udzielonej dobrowolnie i świadomie zgody na przetwarzanie danych osobowych. Odwołanie następuje w formie pisemnej poprzez złożenie oświadczenia administratorowi danych lub osobie upoważnionej do przetwarzania danych

4.2. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

5. Okres przechowywania Pana/Pani danych osobowych.

5.1. Dane osobowe będą 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.

5.2. Po odwołaniu przez Pana/Pani zgody, dane mogą być przechowywane przez Administratora przez okres czasu odpowiadający okresowi przedawnienia roszczeń,

jakie może ponosić Administrator danych i jakie mogą być podnoszone przez Administratora danych. Obecnie okres ten wynosi 10 lat.

6. Odbiorcy danych.

Poza Administratorem Danych Osobowych Pan/Pani dane osobowe mogą zostać udostępnione dla wykonania umowy instytucjom publicznym takim jak ZUS, Urzędy Skarbowe oraz bez Pana/Pani zgody Prokuraturze, Sądom, Komornikom.

7. Prawa osób, których dane dotyczą:

Zgodnie z RODO ma Pan/Pani prawo: dostępu do swoich danych oraz otrzymania ich kopii, do informacji o odbiorcach danych, do usunięcia swoich danych, do sprostowania swoich danych, do przenoszenia danych, do usunięcia danych, ograniczenia przetwarzania danych, do wniesienia skargi do organu nadzorczego.

8. Przekazanie danych do kraju trzeciego.

Administrator *zamierza przekazywać / nie zamierza przekazywać*** Pana/Pani dane/ych osobowe/ych do kraju trzeciego przy spełnieniu warunków zabezpieczenia danych przez kraj trzeci.

9. Informacja o sposobie podania danych.

9.1. Podanie danych może być obowiązkiem wynikającym z przepisów prawa i stanowić warunek zawarcia Umowy Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczególności art. 22 z ind. 1 w związku z art. 94 pkt 9a i 9b,

9.2. Podanie danych może mieć charakter dobrowolny, ale może być konieczne do zawarcia umowy.

10. Przetwarzanie danych do oceny niektórych Pana/Pani cech art.4 ust. 4 RODO.

Pana/Pani dane osobowe mogą być wykorzystane do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się itp.

11. Dane wrażliwe –

Zabrania się przetwarzania danych osobowych ujawniających: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Dopuszcza się przetwarzanie tylko w wyjątkowych sytuacjach zgodnie z art. 9 ust.2 RODO m.in. gdy: osoba, której dane dotyczą wyraziła zgodę, przetwarzanie jest niezbędne do wypełnienia obowiązków i praw przez administratora, do ochrony żywotnych interesów osoby, ze względu na ważny interes publiczny, do celów archiwalnych.

.....
data i podpis osoby zaznajamianej z Klauzulą Informacyjną

*wpisać znak X we właściwe okienko wyboru

** skreślić niewłaściwe

miejsowość,data.....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając w imieniu i na rzecz Administratora Danych Osobowych tj
.....
na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych

i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnie rozporządzenie o ochronie danych DZ.U.UE.L.2016.119.1) – dalej RODO niniejszym **upoważniam:**

Pana/Panią.....
zatrudnioną na stanowisku

do przetwarzania zbioru danych osobowych gromadzonych w aktach osobowych i innych zbiorach, zgodnie z art. 6 RODO, powierzonymi obowiązkami pracowniczymi oraz poleceniami administratora danych. Upoważnienie dotyczy danych osobowych pracowników: obecnych, byłych i przyszłych, przetwarzanych w związku z ich zatrudnieniem jak również kandydatów do pracy w związku z procesem rekrutacji.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi u Administratora Danych Osobowych wewnętrznymi regulacjami w sprawie ochrony danych osobowych. Zakres upoważnienie obejmuje nadanie uprawnień do przetwarzania danych na nośnikach papierowych (zaświadczenia, wydruki itp.) oraz w systemie informatycznym, udostępnionym na stanowisku pracy osoby upoważnionej.

Zobowiązuję osobę upoważniona do zachowania tajemnicy danych osobowych. Tajemnica danych osobowych nie ulega przedawnieniu. Upoważnienie zostaje udzielone na okres zatrudnienia z prawem jego zmiany lub odwołania w każdym czasie. Każda zmiana zakresu obowiązków dołączonych do Umowy o pracę wymaga zmiany upoważnienia.

Naruszenie przepisów RODO może prowadzić do odpowiedzialności administracyjnoprawnej, egzekwowanej przez właściwe organy nadzoru oraz do odpowiedzialności cywilnoprawnej w postępowaniu sądowym prze osobę, której dane dotyczą.

.....
*Podpis osoby upoważnionej
do przetwarzania danych*

.....
podpis Administratora Danych

.....

Rejestr osób upoważnionych do przetwarzania danych osobowych.

1,	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Login	Uwagi
2,						
3,						
4,						
5,						
6,						

.....
Nazwisko i imię

.....
miejscowość i data

.....
adres zamieszkania

**OŚWIADCZENIE O WYRAŻENIU ZGODY
NA PRZETWARZANIE DANYCH OSOBOWYCH**

Zgodnie z art.. 4 ust. 11 RODO Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku 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.U.U.E.L.2016.119.1) – dalej RODO niniejszym świadomie i dobrowolnie **wyrażam zgodę** / **nie wyrażam zgody** * na przetwarzanie moich danych osobowych gromadzonych w aktach osobowych i innych za zasadach określonych w Klauzuli Informacyjnej, udostępnionej przez Administratora Danych Osobowych,

.....
w celu:

.....
Administrator Danych Osobowych zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem. Przetwarzanie będzie odbywać się zgodnie z przepisami RODO i ustawy o ochronie danych osobowych z dnia roku, która jest uzupełnieniem i uszczegółowieniem RODO. Zakres upoważnienie obejmuje nadanie uprawnień do przetwarzania danych na nośnikach papierowych (zaświadczenia, wydruki, wnioski itp.) oraz w systemie informatycznym, udostępnionym na stanowisku pracy osoby upoważnionej.

Powyższe oświadczenie woli może być w każdym czasie odwołane w formie pisemnej poprzez złożenie oświadczenia administratorowi danych lub osobie upoważnionej do przetwarzania danych Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Naruszenie udzielonej powyżej zgody może prowadzić do odpowiedzialności administracyjnoprawnej, egzekwowanej przez właściwe organy nadzoru oraz do odpowiedzialności cywilnoprawnej w postępowaniu sądowym prze osobę, której dane dotyczą.

Oświadczenie jest ważne do czasu zakończenia stosunku pracy.

.....
(podpis upoważniającego)

*wpisać znak X we właściwe okienko wyboru

Zasady obowiązujące pracowników przy przetwarzaniu danych w Krzysztof Pakulski - PPHU ALLTERM -

1. Zasada prywatności kont w systemach (privacy by default).

Zasada ta wprowadza domyślność w ochronie danych. Oznacza to, że w systemach informatycznych pierwotnie mają być wprowadzone najwyższe ustawienia prywatności. Dopiero świadomy wybór użytkownika może obniżyć poziom domyślnych ustawień. W przypadku danych przetwarzanych z użyciem systemów informatycznych, każdy użytkownik takiego systemu powinien być zobowiązany do pracy jedynie na przypisanych mu kontach, które jednoznacznie go identyfikują i wyróżniają. Stosowanie się do tej reguły pozwoli uniknąć anonimowości oraz wątpliwości w zakresie: kto i kiedy ingerował w treść danych lub z ich użyciem pracował. Zmiana tych ustawień powinna następować jedynie na wyraźne żądanie użytkownika oprogramowania/systemu. Osoba, której dotyczą dane, będzie mogła na przykład monitorować ich przetwarzanie.

2. Zasada poufności haseł i kodów dostępu

Każdy użytkownik powinien zachowywać poufność oraz nie przekazywać innym osobom udostępnionych mu haseł i kodów dostępu. Regułą ta dotyczy w szczególności osobistych haseł dostępu do systemów informatycznych, a także kodów dostępu do pomieszczeń. Indywidualne hasło należy zachować jedynie dla siebie. Hasła muszą być utrzymywane w tajemnicy, co oznacza bezwzględny zakaz przekazywania haseł lub udostępniania aktywnej stacji roboczej, umożliwiającej dostęp do systemu informatycznego innym użytkownikom lub osobom trzecim. Nie należy przekazywać ich innym osobom, w tym przełożonemu lub administratorom, a jeśli już do tego doszło to powinno się je niezwłocznie zmienić. Przy wprowadzaniu hasła w obecności osób trzecich, użytkownik powinien wykonać tą czynność w sposób uniemożliwiający tej osobie poznanie wprowadzonego hasła. Zasada ta odnosi się również do haseł tymczasowych/startowych i haseł dostępu, których termin ważności upłynął. Nie należy zapisywać haseł a jeśli zachodzi taka konieczność to musi być ono przechowywane w miejscu w którym nie będzie mogło być odkryte przez osobę nieuprawnioną. Hasła tymczasowe (startowe) przydzielane użytkownikom na początku pracy z systemem muszą być zmieniane podczas pierwszego zarejestrowania się w systemie.

3. Zasada czystego ekranu i czystego pulpitu.

Jest to metoda pozwalająca zabezpieczyć dane w przypadku nieobecności użytkownika (przetwarzającego dane). Zgodnie z tą zasadą każdy komputer służący do pracy z danymi musi mieć ustawiony, włączający się automatycznie po zdefiniowanym okresie bezczynności użytkownika,

wygaszacz ekranu. W przypadku wznowienia aktywności wygaszacz powinien być włączany jedynie po podaniu odpowiedniego hasła. Dodatkowo przed pozostawieniem włączonego komputera bez opieki użytkownicy mogą zablokować go – włączając wygaszacz ekranu lub w przypadku dłuższej nieobecności najlepiej wylogować z systemu. Zasada czystego pulpitu sprowadza się do zapisywania plików w folderach umieszczonych na dysku twardym i nie korzystanie do tego celu z pulpitu. Zapisywanie plików na pulpicie łatwo pozwoli odszukać pliki, aktywność użytkownika a na końcu może doprowadzić do naruszenia ochrony danych osobowych.

4. Zasada zamkniętego pomieszczenia

Opuszczając pomieszczenie służbowe niedopuszczalne jest pozostawienie go niezabezpieczonego, zarówno w godzinach pracy, jak i po jej zakończeniu, jeśli nie pozostaje w nim inna osoba upoważniona. Zasada nie powinna dotyczyć pomieszczeń ogólnie dostępnych takich jak np. salki konferencyjne. Najlepszym rozwiązaniem jest, gdy po zakończeniu dnia pracy, ostatnia wychodząca z pomieszczenia osoba, zamknie wszystkie okna i drzwi oraz zabezpieczy klucze do pomieszczenia zgodnie z obowiązującymi zasadami nadzorowania kluczy.

5. Zasada czystego biurka

Podstawowa zasada osób pracujących z wykorzystaniem dokumentów w formie papierowej. Należy unikać pozostawiania dokumentów na biurku bez nadzoru, szczególnie, gdy dokumenty te zawierają istotne z punktu widzenia Administratora dane. Dokumenty zawierające informacje podlegające ochronie powinny być przechowywane na biurku w taki sposób, aby dostępu do tych dokumentów nie miały osoby nieuprawnione. Dlatego też po zakończeniu pracy wszystkie dokumenty mogące stanowić tajemnicę przedsiębiorstwa, muszą być przechowywane w zamknięciu i nie powinny być ekspozowane w miejscu łatwo dostępnym. Bezwzględnie nie należy zostawiać na wierzchu żadnych dokumentów, kiedy na pewien okres czasu tracimy kontrolę nad nimi (nawet jeśli tylko przechodzimy do innego pokoju). Niepotrzebne w danym momencie dokumenty papierowe i nośniki danych (płyty CD, DVD, pendrive, taśmy) należy bezwzględnie chować w zamkniętych szafach.

6. Zasada czystych drukarek

Drukując dokumenty z użyciem ogólnodostępnej drukarki warto pamiętać, że drukowane informacje powinny być zabierane z drukarek niezwłocznie po wydrukowaniu. Nie należy pozostawiać przy urządzeniach błędnych wydruków. W przypadku nieudanej próby wydrukowania użytkownik powinien skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru.

7. Zasada bezpieczeństwa sprzętu przenośnego.

Korzystanie z urządzeń przenośnych: laptopów, telefonów komórkowych (smartfonów) w miejscach publicznych i innych, nie chronionych, miejscach poza siedzibą firmy wymaga ostrożności, by nie ujawnić osobom nieupoważnionym informacji o danych osobowych. Urządzenia te zbierane z siedziby firmy nie powinny być pozostawiane w samochodzie bądź bez nadzoru w miejscach publicznych. Praca na urządzeniach przenośnych poza firmą niesie ryzyko z uwagi na zabezpieczenia antywirusowe. Przenośne urządzenia powinny być wyposażone w fizyczne zabezpieczenie. Również fakt pracy poza siedzibą firmy wymaga indywidualnej zgody administratora danych.

8. Zasada czystego kosza

W przypadku pracy na dokumentach w formie papierowej, należy pamiętać, że dokumenty papierowe i miękkie nośniki danych z wyjątkiem materiałów jawnych, promocyjnych, marketingowych oraz informacyjnych powinny być niszczone w sposób uniemożliwiający ich ponowne odczytanie np. w niszczarce, umieszczane w specjalnie przeznaczonych do tego celu pojemnikach, spalone, etc.

Powyższe zasady nie wymagają dużego wysiłku, a jedynie systematyki. Stosując je na pewno bezpieczeństwo posiadanych danych się zwiększy, a ich dostępność dla osób nieupoważnionych zostanie znacznie ograniczona.

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:
(zwana dalej „Umową”)

Nazwa firmy przetwarzającej

zwana w dalszej części umowy „**Podmiotem przetwarzającym**”

reprezentowana przez:

oraz

Krzysztof Pakulski - PPHU ALLTERM - zwany w dalszej części umowy „**Administratorem**

danych” lub „**Administratorem**”

reprezentowana przez:

§ 1

Powierzenie przetwarzania danych osobowych.

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „RODO”) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie, a Podmiot przetwarzający zobowiązuje się przetwarzać te dane w sposób zapewniający spełnienie wymogów określonych w Umowie, RODO a także przepisach prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
2. Przez przetwarzanie danych osobowych rozumie się wszelkie operacje wykonywane na danych osobowych, takiej jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie odczytu i usuwanie w rozumieniu art. 4 pkt 2 RODO.
3. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.
5. Niniejsza umowa stanowi integralną część umowy podstawowej nr z dnia/*
6. Dane osobowe przetwarzane w trakcie wykonywania umowy podstawowej nr ...z dnia.... stanowią zbiór danych osobowych, zwany dalej „Zbiorem”.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane /*
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu /**

§3

Obowiązki podmiotu przetwarzającego

1. Przy przetwarzaniu powierzonych danych osobowych, podmiot przetwarzający zobowiązuje się, przy zachowaniu należytej staranności do ich zabezpieczenia poprzez stosowanie odpowiednich

środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.

2. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia, nadając im upoważnienia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
3. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa / zwraca*** Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
4. Podmiot przetwarzający w miarę możliwości, pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
5. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu najpóźniej 24 godzin.
6. Do obowiązków Podmiotu przetwarzającego przed rozpoczęciem przetwarzania powierzonych danych osobowych należy zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń, a w szczególności zabezpieczenie danych przed ich:
 - a) udostępnieniem osobom nieupoważnionym,
 - b) zabranieniem przez osobę nieuprawnioną,
 - c) przetwarzaniem z naruszeniem umowy, przepisów prawa, lub przepisów wewnętrznych Zamawiającego,
 - d) zmianą, utratą, zagubieniem, uszkodzeniem lub zniszczeniem

§4

Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 pkt h) RODO ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Podmiot przetwarzający wyraża zgodę i zobowiązuje się umożliwić Administratorowi kontrolowanie Wykonawcy i jego podwykonawców, w tym pomieszczeń i sprzętu używanego przy przetwarzaniu danych osobowych, w zakresie niezbędnym do stwierdzenia prawidłowości stosowanych zabezpieczeń danych osobowych oraz realizacji obowiązków stąd wynikających, a także w zakresie oceny prawidłowości przetwarzania danych osobowych udostępnionych dla realizacji określonego zadania lub usługi.
3. Przysługujące Administratorowi prawo kontroli realizowane będzie w godzinach pracy Podmiotu przetwarzającego i z minimum 24 godzinnym jego uprzedzeniem.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
5. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w § 5 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem okresu wypowiedzenia.

§8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
 - a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie,
 - b) przetwarza dane osobowe w sposób niezgodny z umową,
 - c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla siedziby Administratora.

Administrator danych

Podmiot przetwarzający

**-należy podać rodzaj danych np. dane zwykłe oraz dane szczególne*

-należy podać kategorię osób, których dane dotyczą np. pracowników

- określić w jakiej postaci np. imion i nazwisk, adresu korespondencji,

*** należy podać cel przetwarzania danych przez podmiot przetwarzający np. realizacji umowy z dnia nr z zakresie danych kadrowych.*

**** wybrać właściwa for*

REJESTR CZYNNOŚCI PRZETWARZANIA

Nazwa i adres **Administradora**

Inspektor Danych Osobowych/*

Lp	Nazwa czynności przetwarzania	cel przetwarzania (art. 30 ust.1 pkt b)	Kategorie osób	kategoria danych	Źródło danych	Planowany termin usunięcia danych art. 30 ust.1pkt.1 f	Nazwa współadministratora i dane kontaktowe (jeśli dotyczy) art. 30 ust.1pkt.1a	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy) art. 30 ust. 1pkt d.	kategorie obiorców innych niż podmiot przetwarzający art. 30 ust.1 pkt d	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32.ust.1	transfer do kraju trzeciego art. Nazwa kraju i podmiotu art.. 30 ust.1 e	jeśli transfer i art. 49 ust. 1 - dokumentacja a odpowiednich zabezpieczeń - art..30 ust.1 e

/* skreślić jeśli nie powołano

kolor żółty – obowiązek wypełnienia

Wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych**w**.....

1,	Wykaz pomieszczeń, w których przetwarzane są dane osobowe (wskazanie konkretnych nr pomieszczeń)	Bud. Pok.
2,	Wykaz pomieszczeń, w których znajdują się komputery stanowiące element systemu informatycznego przetwarzania danych	Bud. Pok.
3,	Wykaz pomieszczeń, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe	Bud. Pok.
4,	Wykaz pomieszczeń archiwum	Bud. Pok.
5,	Wykaz programów, w których przetwarzane są dane osobowe	
6,	Wykaz podmiotów zewnętrznych, które mają dostęp do danych osobowych lub je przetwarzają na podstawie podpisanych umów (np. informatyk) – nazwa firmy, imię, nazwisko, adres, funkcja.	

Wykaz programów informatycznych używanych do przetwarzania danych osobowych

W.....

1,	Program	Dział/ Bud/ Pok.
2,		Dział/ Bud/ Pok.
3,		Dział/ Bud/ Pok..
4,		Dział/ Bud/ Pok.