POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

COMP S.A.

ul. Jutrzenki 116,

02-230 Warszawa

Wersja: 3.0		**Zmiany: -**	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Anna Pietkiewicz Magdalena Sokołowska		Zarząd	05.06.2024r.

CEL I ZAKRES POLITYKI

§ 1

1. Celem Polityki bezpieczeństwa danych osobowych, zwanej dalej „Polityką bezpieczeństwa" lub „Polityką" w Comp S.A., zwanej dalej „Organizacją" bądź „Administratorem Danych", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przetwarzanych w Organizacji przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.
2. W odniesieniu do ochrony danych osobowych stosuje się odpowiednio postanowienia SZBI dotyczące zasad i środków bezpieczeństwa informacji, bądź równoważną politykę stosowaną w Oddziałach Spółki i filiach Oddziałów nie objętych SZBI.
3. W Organizacji przetwarzane są dane osobowe, w szczególności dane osobowe pracowników, kandydatów do pracy, współpracowników, klientów, partnerów biznesowych, dystrybutorów.
4. Dane osobowe są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
5. Polityka bezpieczeństwa obejmuje uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
6. Do stosowania zasad określonych przez Politykę bezpieczeństwa oraz innych z nią związanych dokumentów zobowiązani są pracownicy, współpracownicy Organizacji oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.
7. Naruszenie postanowień niniejszej Polityki może być uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych, uzasadniające rozwiązanie stosunku pracy z winy pracownika, bez zachowania okresu wypowiedzenia lub ważną przyczynę uzasadniającą wypowiedzenie umowy cywilnoprawnej z przyczyn leżących po stronie zleceniobiorcy.

PODSTAWY PRAWNE

§ 2

Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:

a) Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO", „ogólne rozporządzenie o ochronie danych"(Dz. Urz. UE.L nr 119, str.1),

b) Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000 ze zm.) (Ustawa);

c) Systemie Zarządzania Bezpieczeństwem Informacji, przyjętym w Organizacji.

DEFINICJE

§ 3

1. Wyjaśnienie terminów używanych w niniejszej Polityce bezpieczeństwa ochrony danych osobowych.

    1. **Inspektor ochrony danych** / **IOD** – osoba wyznaczona przez administratora danych osobowych na podstawie art. 37. Ust. 4 RODO, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,
    2. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000),
    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 osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119/,
    4. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
    5. **zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
    6. **przetwarzanie danych –** operacja 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.,
    7. **system informatyczny –** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
    8. **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem, zgodnie z SZBI bądź z równoważną polityką stosowaną w Oddziałach Spółki i filiach Oddziałów nie objętych SZBI,
    9. **administrator systemu informatycznego** – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,
    10. **odbiorca –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
    11. **strona trzecia –** 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,
    12. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

13. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
14. **ASI** – Administrator Systemu Informatycznego/ Administratorzy Systemów Informatycznych,
15. **Administrator Danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
16. **dostępność** – właściwość bycia dostępnym i możliwym do wykorzystania na żądanie przez uprawnioną osobę,
17. **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
18. **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
19. **pracownik** – osoba zatrudniona w oparciu o umowę o pracę,
20. **współpracownik** – osoba fizyczna niebędąca pracownikiem, przetwarzająca dane osobowe z upoważnienia Administratora Danych.
21. **rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi i w należyty sposób zweryfikowane,
22. **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
23. **uwierzytelnianie** – dostarczenie zapewnienia, że deklarowana tożsamość jest poprawna,
24. **zgoda osoby, której dane dotyczą** – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli osoby fizycznej, której dane dotyczą, złożone w formie oświadczenia lub wyraźnego działania potwierdzającego, że ta osoba wyraziła zgodę na przetwarzanie dotyczących jej danych osobowych,
25. **użytkownik –** pracownik, współpracownik Organizacji,
26. **SZBI** – System Zarządzania Bezpieczeństwem Informacji, przyjęty w Organizacji,
27. **bezpośredni przełożony** – osoba nadzorująca pracę pracownika/współpracownika.

ADRESACI POLITYKI

§ 4

1. Do stosowania niniejszej Polityki zobowiązane są osoby zatrudnione w Organizacji na podstawie umów o pracę, umów cywilnoprawnych, oraz osoby odbywające praktyki lub staże oraz inne osoby, które Administrator Danych dopuszcza do przetwarzania danych osobowych.

2. Każda z osób wymienionych powyżej zobowiązana jest przestrzegać zasad wskazanych w Polityce oraz przetwarzać dane zgodnie z RODO i odpowiada za bezpieczeństwo przetwarzanych przez siebie danych osobowych.
3. W sytuacji wystąpienia umyślnego bądź nieumyślnego naruszenia zasad przetwarzania danych pracownicy mogą zostać pociągnięci do odpowiedzialności dyscyplinarnej.
4. W szczególnych sytuacjach umyślnego działania na szkodę Administratora pracownicy mogą również zostać pociągnięci do odpowiedzialności karnej, a także może zostać z nimi rozwiązana umowa o pracę bez wypowiedzenia z powodu ciężkiego naruszenia przez pracownika podstawowych obowiązków pracowniczych.

ADMINISTRATOR DANYCH

§ 5

1. Administratorem Danych jest Comp S.A. z siedzibą w Warszawie przy ul. Jutrzenki 116, 02-230 Warszawa, wpisana przez Sąd Rejonowy dla m.st. Warszawy, XIV Wydział Gospodarczy Krajowego Rejestru Sądowego, do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS: 0000037706, NIP: 522-000-16-94, REGON: 012499190.
2. Administrator posiada Odział – Centrum Technologii Sprzedaży, ul. Nawojowska 118, 33-300 Nowy Sącz oraz filię Oddziału – ELZAB, filia Oddziału Centrum Technologii Sprzedaży COMP S.A., ul. Elzab 1, 41-813 Zabrze.
3. Administrator Danych powołuje IOD oraz powołuje, wyznacza i odwołuje ASI.
4. Administrator Danych decyduje o celach i sposobach przetwarzania danych osobowych, zapewniając zgodność tych procesów z RODO.

INSPEKTOR OCHRONY DANYCH

§ 6

1. Funkcję IOD pełni osoba powołana przez Administratora Danych.
2. Administrator Danych może każdorazowo odwołać IOD, z zastrzeżeniem art. 38 RODO.
3. Status Inspektora ochrony danych określony jest w art. 38 RODO.
4. Zgodnie z art. 39 RODO do podstawowych obowiązków Inspektora ochrony danych należy:
    a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    b) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
    d) współpraca z organem nadzorczym;
    e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

§ 7

1. Administrator Danych powołuje ASI oraz wydaje im zalecenia co do sposobu wykonywania obowiązków wynikających z niniejszej Polityki z uwzględnieniem postanowień SZBI bądź równoważnych polityk stosowanych w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI.
2. Administrator Danych wyznacza ASI w stosunku do określonych systemów informatycznych. Jedna osoba może pełnić funkcję ASI w stosunku do jednego lub więcej systemów informatycznych.
3. Bez uszczerbku dla stosownych postanowień SZBI bądź równoważnych polityk stosowanych w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI, do uprawnień i obowiązków ASI należą w szczególności:
    3.1. nadawanie uprawnień do przetwarzania danych osobowych w systemie informatycznym,
    3.2. prowadzenie rejestru nadanych uprawnień do przetwarzania danych w systemie informatycznym,

3.3. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemie informatycznym, a w szczególności przeciwdziałających dostępowi osób niepowołanych do systemu,

3.4. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemem informatycznym, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,

3.5. podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemie informatycznym, zgodnie z SZBI, bądź równoważnych polityk stosowanych w Oddziałach Spółki i filach Oddziałów, nieobjętych SZBI,

3.6. informowanie Administratora Danych i IOD o konieczności wprowadzenia zmian w Instrukcji zarządzania systemem informatycznym (np. z powodu zmian procedur tworzenia kopii zapasowych lub zmiany zabezpieczeń systemu informatycznego),

3.7. sprawowanie nadzoru nad tworzeniem i przechowywaniem kopi zapasowych danych zapisywanych w systemach informatycznych zgodnie z SZBI bądź równoważną polityką stosowaną w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI,

3.8. sprawowanie nadzoru nad stosowaniem środków zabezpieczenia infrastruktury teleinformatycznej zgodnie z SZBI bądź równoważną polityką stosowaną w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI.

4. ASI wykonuje uprawnienia i obowiązki, o których mowa powyżej, w stosunku do infrastruktury teleinformatycznej znajdującej się w danej lokalizacji (w tym serwerów bazodanowych) oraz systemów informatycznych wykorzystywanych przez jej użytkowników.
5. Wykaz osób pełniących funkcję ASI Administrator Danych ogłasza w wewnętrznej sieci internetowej (intranet) lub w inny sposób podaje do wiadomości pracowników.

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 8

1. Administrator Danych, realizując niniejszą Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, którym nadano upoważnienie do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia (w formie tradycyjnej lub e–learningowej do 3 dni od zatrudnienia/ podpisania umowy o współpracy, umowy stażu lub praktyk), o ile zgodnie z umową taka osoba ma uzyskać dostęp do danych osobowych, na wniosek bezpośredniego przełożonego składany w każdej chwili w okresie zatrudnienia. Warunkiem wydania upoważnienia jest zaznajomienie osoby upoważnianej z zasadami ochrony danych osobowych. Pracownik potwierdza fakt zapoznania się z niniejszą Polityką na piśmie (zakres obowiązków i

zobowiązanie do stosowania). Współpracownik zobowiązany jest do podpisania i dostarczenia do IOD stosownego oświadczenia, którego wzór stanowi Załącznik nr 4.

3. Upoważnienia do przetwarzania danych osobowych nadaje Administrator Danych lub pełnomocnik Administratora Danych każdej osobie, która będzie miała dostęp do danych osobowych w związku z wykonywaniem obowiązków służbowych na swoim stanowisku pracy bądź w związku w wykonywaniem umowy o współpracy z Administratorem Danych.
4. Wydawanie oraz cofanie upoważnień do przetwarzania danych osobowych odbywa się na wniosek przy zatrudnieniu lub na wniosek bezpośredniego przełożonego pracownika lub innej osoby nadzorującej wykonywanie czynności przez pracownika / współpracownika w każdym momencie trwania zatrudnienia danej osoby. Wzór wniosku o wydanie / cofnięcie upoważnienia znajduje się w Załączniku nr 3. Wniosek może zostać doręczony do IOD w wersji papierowej bądź z wykorzystaniem poczty e-mail.
5. Upoważnienia do przetwarzania danych osobowych są przechowywane przez IOD w wersji papierowej bądź elektronicznej, a ich kopie znajdują się w teczkach osobowych pracowników. W zakresie współpracowników, upoważnienia przechowuje IOD. Kopie upoważnień wysyłane są również do osób, którym je wydano.
6. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, RODO, postanowieniami niniejszej Polityki oraz zasadami określonymi w SZBI bądź równoważną polityką stosowaną w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI.
7. Obowiązek, o którym mowa w ust. 6 istnieje także po ustaniu zatrudnienia / współpracy. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w Załączniku nr 5.
8. IOD lub osoba wyznaczona przez Administratora Danych prowadzi ewidencję wydanych i cofniętych upoważnień. Ewidencja prowadzona jest wyłącznie w formie elektronicznej.

UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

§ 9

1. Administrator Danych, realizując niniejszą Politykę bezpieczeństwa, dopuszcza, by dane osobowe, których jest administratorem, były przetwarzane poza jego własnymi strukturami organizacyjnymi. Może się to odbywać na drodze powierzenia danego zbioru w określonym celu i zakresie podmiotowi zewnętrznemu, na mocy umowy powierzenia przetwarzania danych osobowych, z zachowaniem wymagań określonych w art. 28 ust. 3 RODO.
2. Powierzenia przetwarzania danych osobowych może dokonać Administrator Danych lub pracownik, posiadający stosowne upoważnienia do zawierania umów w imieniu Administratora Danych. Powierzenie przetwarzania danych osobowych może nastąpić na podstawie pisemnej umowy, aneksu

do umowy lub klauzuli umownej. Za równoważną formę względem pisemnej uznaje się formę elektroniczną z kwalifikowanym podpisem elektronicznym.

3. Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Administratorem powyższych danych są poszczególne podmioty, które obowiązane są do zawarcia pisemnej umowy powierzenia przetwarzania ww. danych. Administrator danych realizuje wówczas zadania podmiotu przetwarzającego, o którym mowa w art. 28 RODO.
4. Zgodnie z przyjętymi zasadami w zakresie obiegu i archiwizacji dokumentów, umowy powierzenia stanowią integralną część umów handlowych/głównych i nie są wyłączane z całości dokumentów, a fakt ich istnienia jest odnotowywany w stosownym systemie informatycznym.

SZKOLENIA Z ZAKRESU DANYCH OSOBOWYCH

§10

1. Obowiązek odbycia szkolenia wstępnego w zakresie ochrony danych osobowych dotyczy każdego pracownika/współpracownika Organizacji, który ma być upoważniony do przetwarzania danych osobowych. Szkolenia mogą być prowadzone z wykorzystaniem platformy e-learningowej.
2. Zakres szkolenia obejmuje również zaznajomienie uczestnika z przepisami RODO, Ustawy, wydanych na jej podstawie aktów wykonawczych oraz wewnętrznymi aktami ochrony danych osobowych, obowiązującymi w Organizacji. Za powyższe odpowiada Dział Kadr w przypadku pracowników. W przypadku współpracowników decyzję w zakresie odbycia szkolenia (co do formy i treści) podejmuje IOD, biorąc pod uwagę charakter współpracy i zakres przetwarzanych danych osobowych.
3. Po ukończeniu szkolenia oraz po zapoznaniu się z zakresem materiału, wskazanym w ust. 2, pracownik/współpracownik informuje o tym fakcie bezpośredniego przełożonego/ osobę nadzorującą wykonywanie czynności przez współpracownika, w celu wystąpienia z wnioskiem o wydanie stosownego upoważnienia do przetwarzania danych osobowych.
4. W przypadku pojawiających się nieprawidłowości lub z uwagi na pojawiające się wątpliwości bądź nowe zadania związane z przetwarzaniem danych osobowych przeprowadza się dodatkowe szkolenie uzupełniające dotyczące zasad ochrony danych osobowych w Organizacji. Decyduje o tym Administrator Danych w porozumieniu z IOD. Szkolenia prowadzone są zgodnie z harmonogramem szkoleń na rok bieżący, przygotowywanym w pierwszym kwartale roku kalendarzowego przez IOD.
5. Istnieje możliwość organizacji szkoleń, które nie zostały uwzględnione w harmonogramie wskazanym w ust. 4. Decyzję o tym podejmuje Administrator Danych w porozumieniu z IOD.
6. Osobą odpowiedzialną za zapewnienie szkoleń i prowadzenie ewidencji przeszkolonych osób jest IOD lub pracownik wyznaczony przez Administratora Danych.

WITRYNY INTERNETOWE

§11

1. Wszelkie kwestie związane z przetwarzaniem danych osobowych z wykorzystaniem witryn internetowych, tj, danych osobowych użytkowników stron internetowych, regulowane są przez odrębne polityki prywatności, zamieszczane na danych stronach internetowych.
2. Polityki wskazane w ust. 1 podlegają bieżącej aktualizacji i cyklicznym przeglądom, dokonywanym przez IOD.

OBOWIĄZEK INFORMACYJNY

§12

1. Organizacja przestrzega zasady realizacji obowiązku informacyjnego, zgodnie z art. 13 – 14 RODO.
2. Celem wykonania obowiązku wskazanego w ust. 1, kierowana w imieniu Organizacji do osób trzecich korespondencja handlowa, w tym oferty, zapytania ofertowe, projekty umów, zamówienia, winny być opatrzone stosowną klauzulą informacyjną zaczerpniętą z zasobów Intranetu Organizacji.
3. Odpowiedzialność za realizację obowiązku wskazanego w ust. 1 w konkretnym przypadku ponosi osoba prowadząca daną korespondencję.

AUDYTY

§13

1. Audyty bezpieczeństwa danych osobowych w zakresie stosowanych zabezpieczeń prowadzone są raz w roku przez IOD, wyznaczonego pracownika lub podmiot zewnętrzny, wyznaczony przez Administratora Danych.
2. Audyty obejmują kwestie stosowanych zabezpieczeń organizacyjnych, tj. realizacji przyjętych postanowień co do bezpieczeństwa danych osobowych i zasad ich przetwarzania. Audyty obejmują zagadnienia uwzględnione w planie audytu na dany rok kalendarzowy. Przynajmniej raz na 3 lata audyt dotyczy wszystkich aspektów związanych z bezpieczeństwem danych osobowych i ma charakter audytu potwierdzającego zgodność przyjętych w Organizacji regulacji z RODO.
3. Audyty w zakresie zabezpieczeń technicznych, z uwagi na wymogi SZBI bądź równoważnej polityki stosowanej w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI, odbywają się zgodnie z przyjętymi tamże regulacjami i wypełniają znamiona audytu w zakresie bezpieczeństwa danych osobowych. Jeżeli SZBI bądź wskazana w zdaniu poprzednim polityka równoważna nie obejmuje całej Organizacji, IOD podejmuje stosowną decyzję w zakresie formy planowego audytu w tej część, w której nie wdrożono

SZBI bądź polityce równoważnej, uwzględniając terminy oraz wymagania bezpieczeństwa względem danych osobowych, zawarte we wskazanych powyżej politykach , które stosuje się odpowiednio.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

§ 14

1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń, są wszyscy użytkownicy.
2. Każdy użytkownik jest zobowiązany do niezwłocznego poinformowania IOD oraz właściwego ASI odpowiadającego za dany system o każdym przypadku złamania zasad przetwarzania danych, a w szczególności o sytuacjach udostępnienia danych osobom nieuprawnionym.
3. ASI, który wykrył lub został poinformowany o nieprawidłowościach przy przetwarzaniu danych osobowych, powinien zgłosić incydent bezpieczeństwa informacji i podjąć jego obsługę zgodnie z SZBI bądź równoważną polityką stosowaną w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI.
4. Bez uszczerbku dla stosownych i dalej idących postanowień SZBI bądź równoważnej polityki stosowanej w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI, za naruszenie ochrony danych osobowych uważa się w szczególności:
   4.1. nieuprawniony dostęp lub próbę dostępu do systemu lub pomieszczeń, w których następuje proces przetwarzania danych (widoczne uszkodzenia bądź naruszenia zabezpieczeń);
   4.2. naruszenie lub próbę naruszenia zbioru danych oraz integralności systemu;
   4.3. nieautoryzowane zniszczenie lub próbę zniszczenia danych zgromadzonych w zbiorach papierowych i/lub systemie;
   4.4. zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany;
   4.5. nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);
   4.6. inny stan systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem;
   4.7. stwierdzenie, że stan dokumentacji lub stan pomieszczeń bądź szaf biurowych, w których przechowywana jest dokumentacja, wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby nieupoważnione.
5. W przypadku stwierdzenia naruszenia danych w systemie informatycznym lub zaistnienia okoliczności wskazujących na naruszenie zabezpieczeń systemu informatycznego, w którym przetwarzane są dane osobowe, użytkownik zobowiązany jest do postępowania zgodnie z zasadami SZBI, bądź

równoważonej polityki stosowanej w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI oraz bezzwłocznego powiadomienia o tym fakcie właściwego ASI oraz IOD.

6. Bez uszczerbku dla stosownych postanowień SZBI oraz równoważnej polityki stosowanej w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI – PBI , w szczególności zawarte w procedurze SZBI PSQ.09.7 – Zasady obsługi incydentów bezpieczeństwa, punkt 4.11. Postępowanie Użytkowników w wypadku wystąpienia zdarzenia bądź incydentu, do czasu przybycia IOD lub ASI bądź osoby upoważnionej przez niego, użytkownik:
   6.1. zabezpiecza dostęp do miejsca lub urządzenia;
   6.2. wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane;
   6.3. podejmuje, stosownie do zaistniałej sytuacji, inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
7. Bez uszczerbku dla stosownych postanowień SZBI bądź równoważnej polityki stosowanej w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI, ASI, w obecności IOD, po przybyciu na miejsce, w którym doszło do naruszenia ochrony danych osobowych:
   7.1. ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe, stan urządzeń i zbioru danych;
   7.2. zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia, jak również sprawdza zawartość zbioru danych osobowych;
   7.3. sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych;
   7.4. sprawdza sposób działania programu (w tym również obecność wirusów komputerowych);
   7.5. ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu;
   7.6. niezwłocznie zapewnia przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia baz danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności;
   7.7. sprawdza jakość komunikacji w systemie informatycznym;
   7.8. dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych wskutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych;
   7.9. spisuje relację osoby zatrudnionej przy przetwarzaniu danych, która dokonała powiadomienia;
   7.10. podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych i w przypadkach uzasadnionych niezwłocznie powiadamia Administratora Danych lub właściwą osobę podejmującą decyzję w imieniu Administratora Danych;
   7.11. sporządza raport zawierający w szczególności: dane personalne osoby, która stwierdziła naruszenie, datę i godzinę powiadomienia, opis podjętych czynności i ich uzasadnienie.

REJESTRY I ANALIZA RYZYKA

§ 15

1. Administrator Danych prowadzi następujące Rejestry: Rejestr Czynności Przetwarzania Danych Osobowych oraz Rejestr Kategorii Czynności Przetwarzania.
2. Rejestr Czynności Przetwarzania Danych Osobowych prowadzony jest w oparciu o informacje przesyłane do IOD przez Dyrektorów/Kierowników Działów/Biur i uwzględnia czynności charakterystyczne dla danej jednostki, oparte na przetwarzaniu danych osobowych. Rejestr Kategorii Czynności Przetwarzania uwzględnia zbiory danych, względem których Organizacja występuje w roli procesora i prowadzony jest z uwzględnieniem podziału na Działy/Biura.
3. Osobą odpowiedzialną za prowadzenie i aktualizację Rejestrów jest IOD lub inna osoba wyznaczona przez Administratora Danych.
4. Dla każdej czynności, uwzględnionej w Rejestrze Czynności Przetwarzania Danych Osobowych przeprowadzana jest Analiza Ryzyka, zgodnie ze wzorem przesłanym do Dyrektorów/Kierowników Działów/Biur. Aktualizacja Analizy Ryzyka następuje wraz z aktualizacją Rejestru Czynności Przetwarzania Danych Osobowych i jest sporządzana przez Dyrektorów/Kierowników Działów/Biur, przy współpracy z IOD lub inną osobą, wyznaczoną przez Administratora Danych. Aktualizacja Rejestru Kategorii Czynności Przetwarzania Danych Osobowych opiera się na tych samych zasadach.
5. Administrator Danych, zgodnie z art. 32 ust. 1 lit. d RODO zdecydował o wprowadzeniu Procedury, która pozwoli na regularne testowanie i mierzenie zastosowanych zabezpieczeń. W przedmiotowej Procedurze uwzględniono zabezpieczenia organizacyjne, które zastosował Administrator Danych, a także terminy i sposoby ich weryfikacji. Za realizację powyższego odpowiada IOD lub inna osoba wyznaczona przez Administratora Danych.

ZASADY BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 16

1. Wszelkie procedury i działania związane z zapewnieniem bezpieczeństwa danych osobowych podejmowane są w oparciu o SZBI bądź równoważną polityką stosowaną w Oddziałach Spółki i filiach Oddziałów, nie objętych SZBI.

ZMIANY W POLITYCE

§ 17

1. Zmiany Polityki, nie wprowadzające nowych praw i obowiązków dla pracowników Organizacji, a jedynie mające charakter porządkowy, nie wymagają uregulowania w odrębnej uchwale i wprowadzane są na bieżąco przez Inspektora Ochrony Danych. Każdorazowo Inspektor publikuje zmiany w Intranecie i komunikuje pracownikom zakres wprowadzonych aktualizacji.

ZAŁĄCZNIKI

Załącznik nr 1 - Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których Administrator przetwarza dane osobowe,

Załącznik nr 2 - Wykaz zbiorów wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

Załącznik nr 3 - Wzór wniosku o wydanie/cofnięcie upoważnienia,

Załącznik nr 4 – Wzór oświadczenia o zapoznaniu się z Polityką (dla współpracowników),

Załącznik nr 5 - Wzór upoważnienia do przetwarzania danych osobowych,

Załącznik nr 6 - Wzór instrukcji postępowania w przypadku zgłoszenia naruszenia ochrony danych osobowych,

Załącznik nr 7 - Wzór instrukcji postępowania w przypadku zgłoszenia wniosku o realizację prawa „bycia zapomnianym”,

Załącznik nr 8 - Wzór instrukcji postępowania w przypadku zgłoszenia wniosku w przedmiocie dostępu do danych, sprostowania, modyfikacji ii ograniczenia przetwarzania.

Dokument sporządzono:	**Pełen podpis Administratora Danych:**	**Pieczęć**
Data: 05.06.2024r. Miejsce: Warszawa	**Uchwała nr 5 Zarządu Comp S.A. w Warszawie z dnia 05.06.2024r. w sprawie przyjęcia nowej Polityki Bezpieczeństwa Danych Osobowych w Spółce Comp S.A.**	

	Nazwa podmiotu	Adres	Uwagi
Dane osobowe przetwarzane jako Administrator Danych	**COMP S.A.**	ul. Jutrzenki 116, 02-230 Warszawa	Lokalizacje i budynki, w których przetwarzane są dane osobowe: **1) COMP S.A. Centrala** ul. Jutrzenki 116 oraz ul. Jutrzenki 118, 02-230 Warszawa **2) COMP S.A. Centrum Usług** ul. Działkowa 115A, 02-234 Warszawa **3) COMP S.A. Oddział Centrum Technologii Sprzedaży** ul. Nawojowska 118,

			33-300 Nowy Sącz **4) Filie COMP S.A. Centrum Usług:** **Filia Białystok** ul. Ciołkowskiego 24, 15-545 Białystok **Filia Gdańsk** ul. Budowlanych 46 A, 80-298 Gdańsk **Filia Katowice** ul. Ks. Bpa. Bednorza 2a-6, Budynek „E”, 40-384 Katowice **Filia Kraków** ul. Halicka 9, 31-036 Kraków **Filia Lublin** ul. Wojciechowska 9A, 20-704 Lublin **Filia Łódź**

			ul. św. Teresy 91, 91-341 Łódź **Filia Olsztyn** ul. Augustowska 23A, 10-683 Olsztyn **Filia Poznań** ul. Polańska 1, 61-614 Poznań **Filia Rzeszów** ul. Hoffmanowej 19, 35-016 Rzeszów **Filia Szczecin** ul. Milewskiego 2A, 71-477 Szczecin **Filia Wrocław** Al. Armii Krajowej 61, 50-541 Wrocław 5) Centrum przetwarzania danych Comp w kolokacji Netia **Jawczyce ul. Sadowa 5**

			Stan na dzień wdrożenia Dokumentacji ochrony danych osobowych. Zawsze aktualna lista filii COMP S.A. Centrum Usług znajduje się na stronie internetowej: http://www.comp.com.pl/oferta/uslugi-it/kontakt **6) Filie COMP S.A. – Centrum Technologii Sprzedaży:** **Serwis Centralny w Nowym Sączu** ul. Nawojowska 118, 33-300 Nowy Sącz **Oddział Serwisu w Gdańsku** ul. Chłopska 72, 80-350 Gdańsk

			Oddział Serwisu w Dąbrowie Górniczej ul. Piłsudskiego 6, 41-303 Dąbrowa Górnicza **Oddział Serwisu we Wrocławiu** Al. Armii Krajowej 61, 50- 541 Wrocław **Oddział Serwisu w Warszawie** ul. Działkowa 115A, 02-234 Warszawa **Oddział Serwisu w Poznaniu** ul. Sieradzka 24 lok 3, 60-163 **Filia Działu Usług Systemowych** (Helpdesk) zlokalizowana w 33-300 Nowy Sącz Ul. Wiśniowieckiego 138

			Stan na dzień wdrożenia Dokumentacji ochrony danych osobowych. Zawsze aktualna lista filii COMP S.A. Oddział Centrum Technologii Sprzedaży znajduje się na stronie internetowej: http://www.novitus.pl/pl/serwis.html ELZAB, filia Oddziału Centrum Technologii Sprzedaży Comp S.A. Centrala (biurowiec Elzabu, Zabrze): ul. ELZAB 1, 41-813 Zabrze. Biura handlowe i serwisy:

			ul. Krakowiaków 2, 02-255 Warszawa; ul. Akacjowa 4, 62-005 Suchy Las k/Poznania; ul. Słubicka 22 53-615 Wrocław.

nr 2 – Wykaz zbiorów wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Nr	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych
1.	**Rekrutacja**	system poczty e-mail	Dane osobowe przetwarzane w celu zmierzającym do zawarcia umowy, podjęcia zatrudnienia w COMP S.A.	Osoby ubiegające się o zatrudnienie w COMP S.A.	Imię (imiona), nazwisko, imiona rodziców, data urodzenia, obywatelstwo, miejsce zamieszkania (adres do korespondencji), wykształcenie (nazwa szkoły i rok jej ukończenia, zawód, specjalność, stopień naukowy, tytuł zawodowy, tytuł naukowy), wykształcenie uzupełniające (kursy, studia podyplomowe, data ukończenia nauki lub data rozpoczęcia nauki w przypadku jej trwania), przebieg dotychczasowego zatrudnienia (okresy zatrudnienia u kolejnych pracodawców oraz zajmowane stanowiska pracy), dodatkowe uprawnienia, umiejętności, zainteresowania (np. stopień znajomości języków obcych, prawo jazdy, obsługa komputera), dowód osobisty / inny dowód tożsamości (seria, numer, wydany przez), inne informacje ujawnione w dokumentach aplikacyjnych (m.in. CV lub liście motywacyjnym), historia zatrudnienia w COMP S.A. (rodzaj umowy, wynagrodzenie, wymiar czasu pracy), proponowane warunki zatrudnienia, wyniki badań medycyny pracy.
2.	**Pracownicy i współpracownicy**	Symfonia, SAP, Płatnik, system poczty e-mail,	Dane osobowe przetwarzane w związku ze świadczeniem przez pracowników pracy oraz usług na rzecz COMP	Pracownicy zatrudnieni na podstawie umów o pracę oraz umów cywilnoprawnych (w tym praktykanci), oraz B2B, członkowie organów COMP S.A.	Imię (imiona), nazwisko, imiona rodziców, data urodzenia, obywatelstwo, miejsce zamieszkania (adres do korespondencji), wykształcenie (nazwa szkoły i rok jej ukończenia, zawód, specjalność, stopień naukowy, tytuł zawodowy, tytuł naukowy), wykształcenie uzupełniające (kursy, studia podyplomowe, data ukończenia nauki lub data rozpoczęcia nauki w przypadku jej trwania), przebieg dotychczasowego zatrudnienia (okresy zatrudnienia u kolejnych

		hit (help desk IT) Q-Inwentarz, EOD (kontakty do pracowników AD (kontakty do pracowników Unicard (rejestracja czasu pracy, RCP) Office 365, w tym Teams ERP Impuls Aurora (dział mechaniczny ELZAB) WK 16 Projektron Mantis	S.A. oraz w celu wypełnienia obowiązków wynikających z przepisów prawa.	oraz byli pracownicy i współpracownicy.	pracodawców oraz zajmowane stanowiska pracy), dodatkowe uprawnienia, umiejętności, zainteresowania (np. stopień znajomości języków obcych, prawo jazdy, obsługa komputera), PESEL, NIP i REGON (w przypadku osób prowadzących własną działalność gospodarczą), numer rejestracyjny pojazdu, stan rodzinny (imiona i nazwiska oraz daty urodzenia dzieci), powszechny obowiązek obrony (stosunek do powszechnego obowiązku obrony, stopień wojskowy, numer specjalności wojskowej, przynależność ewidencyjna do WKU, numer książeczki, przydział mobilizacyjny do sił zbrojnych RP), osoba, którą należy zawiadomić w razie wypadku (imię, nazwisko, adres, telefon), nazwa Urzędu Skarbowego, Oddział NFZ, rachunek bankowy (nazwa banku, numer konta), dowód osobisty / inny dowód tożsamości (seria, numer, wydany przez), miejsce zameldowania, warunki zatrudnienia (rodzaj umówionej pracy, miejsce wykonywania pracy, wymiar czasu pracy, wynagrodzenie, inne składniki wynagrodzenia, inne warunki zatrudnienia), dzień rozpoczęcia pracy, dzień zakończenia pracy, stanowisko, pion / wydział / dział, urlopy (rodzaj, wymiar), oświadczenia zleceniobiorcy / wykonawcy: o byciu/nie byciu pracownikiem w innym zakładzie pracy z wynagrodzeniem powyżej / poniżej minimalnego wynagrodzenia za pracę, osobą niepracującą, zarejestrowaną w Urzędzie Pracy, emerytem / rencistą, emerytem / rencistą pracującym, zatrudnionym na umowę zlecenie w innym zakładzie pracy, właścicielem / wspólnikiem firmy ubezpieczonym w ZUS, uczniem / studentem, praktykanci: legitymacja studencka (numer, wydana przez), nazwa uczelni oraz kierunek i rok studiów, oświadczenie dla celów częściowego zaniechania poboru zaliczki na podatek dochodowy od osób fizycznych (w tym przewidywane dochody małżonka / dziecka), oświadczenie dla celów stosowania obniżonych kosztów uzyskania przychodów (w tym informacja o zamieszkiwaniu poza miejscowością, w której znajduje się zakład pracy, informacja o nieotrzymywaniu dodatku za

		Samba			rozłąkę), oświadczenie o byciu rodzicem dziecka do lat 14, oświadczenie dla celów naliczania miesięcznych zaliczek na podatek dochodowy od osób fizycznych (w tym informacje o nieotrzymywaniu emerytury lub renty za pośrednictwem płatnika, nieosiąganiu dochodów z tytułu członkostwa w rolniczej spółdzielni produkcyjnej lub innej spółdzielni zajmującej się produkcją rolną, nieotrzymywanie świadczeń pieniężnych wypłacanych z Funduszu Pracy lub z Funduszu Gwarantowanych Świadczeń Pracowniczych, nieosiąganiu dochodów z działalności gospodarczej lub z najmu lub dzierżawy), członkowie rodziny (imię (imiona), nazwisko, data urodzenia, miejsce zamieszkania, PESEL, stopień pokrewieństwa, adres e-mail, telefon domowy, telefon komórkowy, główna miejscowość opieki zdrowotnej), wizerunek, dane związane z użytkowaniem i lokalizacją pojazdów służbowych (lokalizacja GPS).
3.	**Baza - Rozporządzenie MAR**	system poczty e-mail	Dane osobowe przetwarzane w celu wypełnienia przez COMP S.A. jako spółki publicznej notowanej na Giełdzie Papierów Wartościowych w Warszawie S.A., obowiązków wynikających z przepisów prawa.	Osoby posiadające dostęp do informacji poufnej, osoby pełniące obowiązki zarządcze, osoby blisko związane (w rozumieniu art. 3 ust. 1 pkt 26) Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku oraz uchylającego	Osoba posiadająca dostęp do informacji poufnej – imię, nazwisko, nazwisko rodowe, funkcja, numer telefonu służbowego (stacjonarnego, komórkowego), adres e-mail, data urodzenia, PESEL, prywatny numer telefonu, adres zamieszkania (pełny), informacja, do której uzyskano dostęp, data i godzina uzyskania dostępu do informacji poufnej. Osoba pełniąca obowiązki zarządcze – imię, nazwisko, nazwisko rodowe, funkcja, numer telefonu służbowego (stacjonarnego, komórkowego), adres e-mail, data urodzenia, PESEL, prywatny numer telefonu, adres zamieszkania (pełny), data rozpoczęcia pełnienia funkcji zarządczej, data zakończenia pełnienia funkcji zarządczej. Osoba blisko związana – imię, nazwisko oraz funkcja osoby po stronie emitenta (COMP S.A.), która wskazuje osobę blisko związaną, imię, nazwisko, nazwisko rodowe, rodzaj / typ

				dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE).	powiązania, data powstania powiązania (np. data urodzenia dziecka, data zawarcia związku małżeńskiego, data powołania w skład organu), data wygaśnięcia powiązania (np. data zgonu, data ustania związku małżeńskiego, data odwołania ze składu organu), adres e-mail, data urodzenia, PESEL, prywatny numer telefonu, adres zamieszkania (pełny), imię, nazwisko przedstawiciela ustawowego osoby blisko związanej (np. matka, ojciec, opiekun).
4.	**Klienci** **(Centrala)**	Symfonia, Market, system poczty e-mail, EOD	Dane osobowe przetwarzane w celu realizacji zawartych z klientami umów.	Klienci oraz potencjalni klienci Oddziału IT (przedstawiciele, osoby reprezentujące, osoby kontaktowe).	Imię, nazwisko, firma, stanowisko, nr telefonu, adres e-mail, nr fax, NIP, Regon, nr KRS, siedziba, adres prowadzenia działalności (nr domu, nr lokalu, ulica, miasto, województwo, kraj, kod pocztowy) numer rachunku bankowego, symbol banku, nazwa banku, numer faktury, kwota zobowiązania,

5.	**Klienci (PSS)**	System OTRS **Baza: https://webinaria.comp.com.pl/** EOD	Dane osobowe przetwarzane w celu realizacji zawartych z klientami umów serwisowych. Dane osobowe przetwarzane w celu realizacji seminariów, webinariów, eventów, spotkań Umowy, kontrakty handlowe	Obecni Klienci (tylko Klienci Pionu PSS) (przedstawiciele, osoby reprezentujące, osoby kontaktowe). Klienci oraz potencjalni klienci całej GK COMP (przedstawiciele, osoby reprezentujące, osoby kontaktowe). j.w.	Imię, nazwisko, firma, stanowisko, nr telefonu, adres e-mail, nr fax, NIP, Regon, nr KRS, siedziba, adres prowadzenia działalności (nr domu, nr lokalu, ulica, miasto, województwo, kraj, kod pocztowy) – jeżeli jest podana przez Klienta stopka adresowa w mailu. Imię, nazwisko, firma, stanowisko, nr telefonu, adres e-mail, nr fax, NIP, Regon, nr KRS, siedziba, adres prowadzenia działalności (nr domu, nr lokalu, ulica, miasto, województwo, kraj, kod pocztowy) j.w.
6.	**Klienci Oddziału Centrum Technologii Sprzedaży**	SAP, Elektroniczny Obieg Dokumentów (Business nawigator Oddział),	Dane osobowe przetwarzane w celu realizacji zawartych z klientami umów oraz w celu wypełnienia obowiązków wynikających	Klienci oraz potencjalni klienci COMP S.A. Oddział Centrum Technologii Sprzedaży, w tym klienci Pionu Centrum Usług (przedstawiciele, osoby reprezentujące, osoby kontaktowe, osoby	Imię, nazwisko, firma, stanowisko, nr telefonu, adres e-mail, nr fax, NIP, Regon, nr KRS, siedziba, adres prowadzenia działalności (nr domu, nr lokalu, ulica, miasto, województwo, kraj, kod pocztowy) numer rachunku bankowego, symbol banku, nazwa banku, numer faktury, kwota zobowiązania, dane klienta końcowego – użytkownika (imię, nazwisko, adres, nr tel., nr tel. komórkowego, e-mail).

		CMS Novitus, Extranet system poczty e-mail NSU Novitus Extranet / Mplatform Baza Novitus SQL Baza SQL / cyber_Folks SDF1 / Oktawave SDF3 / Oktawave NoviCloud / Oktawave Salesmanago / Benhauer	z przepisów prawa.	fizyczne prowadzące własną działalność gospodarczą, osoby fizyczne) oraz klienci końcowi – użytkownicy.	
	Klienci i dealerzy ELZAB	ISOPH Office 365	Zawieranie i realizacja umów z klientami i partnerami	Klienci i ich przedstawiciele, partnerzy handlowi ELZAB (dealerzy) i ich	Firma przedsiębiorcy (Partnera), oznaczenie formy prawnej, adres prowadzenia działalności gospodarczej, Numer Identyfikacji Podatkowej, numer firmy w systemie informatycznym ELZAB (nr SAP), numer umowy o współpracy

		SAP ERP Intranet Systemy producenta mojakasa.online, w tym powiązane mikroserwisy, oprogramowanie deweloperskie: kompilatory środowiska, debuggery, programy narzędziowe, narzędzia deweloperskie do profilowania kodu Business Navigator (obieg dokumentów ELZAB)	(dealerami) ELZAB Realizacja czynności związanych z obsługą napraw, serwisu, rozliczeń, raportowania; czynności związane z obsługą klienta.	przedstawiciele, w tym użytkownicy Portalu Serwisanta (ISOPH) oraz osoby działające w imieniu partnerów (Serwisanci), potencjalni klienci, użytkownicy strony internetowej	z ELZAB, data podpisania umowy o współpracy z ELZAB, imiona i nazwiska osób reprezentujących firmę, status firmy (Partnera) w ELZAB (określa poziom przypisanego rabatu handlowego), wielkość obrotów w danym roku kalendarzowym, minimalny obrót kwartalny i roczny konieczny do utrzymania statusu, wielkość limitu kredytowego w ELZAB, suma zobowiązań z podziałem na przeterminowane i nieprzeterminowane, dane do kontaktu, imię i nazwisko handlowców ELZAB przypisanych do regionu Partnera, dane do kontaktu do handlowców ELZAB, w przypadku danych do umowy: nazwiska i imiona, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, dane kontaktowe (e-mail i nr telefonu), pod współpracę z Uber i Uber Partner dodatkowo: dane dotyczące transakcji i przejazdu, w tym trasa przejazdu (jedynie odległość, bez konkretnych lokalizacji). Nagrania rozmów, w przypadku połączeń na nr stacjonarne ELZAB (Centralka Slican - moduł do nagrywania to Fontel Klient). Do fiskalizacji kas niezbędne są NIP podatnika, dane podatnika oraz stawki podatkowe. Przetwarzane są także powiązane dane, w tym historia transakcji, należności, kwoty podatku oraz szczegóły dotyczące umowy z partnerem.
7.	**Kontrahenci**	Elektroniczny Obieg Dokumentów	Dane osobowe przetwarzane	Dostawcy produktów i usług oraz inne osoby	Imię, nazwisko, firma, stanowisko, nr telefonu, adres e-mail, nr fax, NIP, PESEL, Regon, nr KRS, numer i seria dowodu osobistego, przez kogo wydany i kiedy, siedziba, adres

		(Business nawigator Oddział), SAP, Microsoft Dynamics (CRM), CMS Novitus, CMS Centrala Extranet, Novitus Friends Club, system poczty e-mail, EOD_Ready – Centrala Jutrzenki Symfonia – Centrala Jutrzenki Business Navigator, Portal Dealera,	w celu realizacji zawartych z kontrahentam i umów oraz w celu wypełnienia obowiązków wynikających z przepisów prawa. Zapewnienie obsługi magazynu i łańcucha dostaw, realizacja umów.	wykonujące usługi na rzecz COMP S.A., w tym: • podmioty świadczące usługi serwisowe, m.in. podmioty świadczące usługi jako APS; • podmioty prowadzące serwis kas; • podmioty prowadzące serwis kas oraz sprzedaż kas. • Pozostali kontrahenci ELZAB, osoby uprawnione do ich reprezentacji i kontaktu, dostawcy, kurierzy i ich przedstawiciele, adresaci i nadawcy	prowadzenia działalności oraz adres zamieszkania w zakresie: nr domu, nr lokalu, ulica, miasto, województwo, kraj, kod pocztowy) numer rachunku bankowego, symbol banku, nazwa banku, numer faktury, kwota zobowiązania, Urząd Skarbowy, numer rejestracji w KRS, dane kontaktowe, stanowisko reprezentanta, W przypadku obsługi magazynu ELZAB, przetwarzanie danych osobowych występuje w zakresie wynikającym z potrzeb transportowych. W ramach dowodów audytowych dostarczono przykład listy załadunkowej na wyjazd, gdzie wskazane są nr zlecenia, adres dostawy (częściowo - adresy osób prowadzących jednoosobową działalność gospodarczą), a także numery przesyłek (kartonów). Wszystko generowane z systemu WMS. W ramach protokołu przekazania towaru przetwarzane są nazwa firmy, adres, NIP lub zagraniczny odpowiednik, telefon / fax oraz imię i nazwisko osoby kontaktowej, jak również dane dotyczące przesyłki, w tym jej wartość i waga.

		Portal Serwisanta			
8.	**Lista serwisantów kas**	SAP system poczty e-mail	Dane osobowe przetwarzane w celu wypełnienia obowiązków wynikających z przepisów prawa.	Osoby fizyczne wykonujące serwis kas na warunkach określonych w Rozporządzeniu Ministra Finansów z dnia 14 marca 2013 r. w sprawie kas rejestrujących (Dz. U. z 2013, poz. 363).	imię, nazwisko, PESEL, wizerunek (zdjęcie)
9.	**Lista gości**	Baza kontaktów system poczty e-mail	Dane osobowe przetwarzane w celach marketingowych i wizerunkowych.	Osoby zapraszane na spotkania branżowe, imprezy firmowe, adresaci kartek okolicznościowych oraz upominków wysłanych przez COMP S.A.	imię, nazwisko, nazwa firmy, stanowisko, e-mail, adres korespondencyjny (służbowy i prywatny), nr telefonu (służbowy i prywatny),
10	**Baza marketingowa, dane przetwarzane przez strony internetowe**	Microsoft Dynamics (CRM), CMS Novitus Salesmanago / Benhauer	Dane osobowe przetwarzane w celach marketingowych.	Odbiorcy mailingów, użytkownicy usługi newsletter oraz adresaci wszelkich innych działań marketingowych.	imię, nazwisko, numer telefonu, adres e-mail, adres korespondencyjny Dane o wykorzystaniu strony przez użytkownika, w tym identyfikatory internetowe; dane podawane w ramach zostawianych wiadomości i formularzy kontaktowych.

		system poczty e-mail Strony internetowe ELZAB			
11.	**Dane powierzone** **(Centrala)**	-	Dane osobowe przetwarzane w celu realizacji zawartych z klientami umów.	Osoby, których administratorem ich danych są inne podmioty - klienci COMP S.A., w szczególności klienci Oddziału IT na rzecz, których COMP S.A. świadczy usługi informatyczne w zakresie wdrożenia, wsparcia czy utrzymania systemów informatycznych, jak również klienci mojakasa.online (filia ELZAB).	wszelkie kategorie danych jakie mogą się znajdować w systemach klientów oraz w systemie mojakasa.online
12.	**Rejestr korespondencji** **(Oddział Centrum Technologii Sprzedaży)**	Microsoft Dynamics (CRM) Elektroniczny Obieg Dokumentów	Dane osobowe przetwarzane w celu bieżącej obsługi biura.	Nadawcy i odbiorcy korespondencji wychodzącej oraz przychodzącej w tym przesyłek kurierskich.	Imię (imiona), nazwisko, firma, adres, data, przedmiot korespondencji, dział i inicjały odbiorcy.

		(Business nawigator Oddział Koresponden cja przychodząc a – książka papierowa			
13.	**Rejestr korespondencji (Centrala)**	Elektroniczny Obieg Dokumentów	Dane osobowe przetwarzane w celu bieżącej obsługi Spółki, w tym umowy, pisma i inne.	Klienci oraz potencjalni klienci Spółki (przedstawiciele, osoby reprezentujące, osoby kontaktowe), przedstawiciele i pracownicy instytucji państwowych, społecznych i organów ścigania.	Imię, nazwisko, firma, stanowisko, nr telefonu, adres e-mail, nr fax, NIP, PESEL, Regon, nr KRS, nr rejestracyjny pojazdu, nr dowodu osobistego, przez kogo wydany i kiedy, siedziba, adres prowadzenia działalności oraz adres zamieszkania w zakresie: nr domu, nr lokalu, ulica, miasto, województwo, kraj, kod pocztowy) numer rachunku bankowego, symbol banku, nazwa banku, numer faktury, kwota zobowiązania, Urząd Skarbowy
14.	**Ewidencja osób wchodzących** **(Centrala i Centrum Usług)**	System KD	Dane osobowe (pracownik i gość) przetwarzane w celu zapewnienia bezpieczeństwa i porządku na terenie obiektów COMP S.A. (w tym poszczególnych pomieszczeń –	Osoby wchodzące / wjeżdżające na teren obiektów COMP S.A.	Imię (imiona), nazwisko, godzina wejścia, godzina wyjścia, powód, numer legitymacji służbowej, dowód osobisty (numer, seria, wydany przez), numer rejestracyjny pojazdu. Zdjęcie do identyfikatora (karta systemu KD) – dla pracowników.

			dot. strefy bezpieczeństwa).		
15.	**Monitoring** **(Centrala i Oddział oraz filia ELZAB)**	-	Dane osobowe przetwarzane w celu zagwarantowania bezpieczeństwa osób przebywających na obszarze objętym monitoringiem	Osoby przebywające w obszarze objętym monitoringiem	Wizerunek osoby fizycznej
16.	**System Alarmowy** **(Centrala i Centrum Usług)**	SWiN	Dane osobowe przetwarzane w celu zapewnienia bezpieczeństwa fizycznego stref chronionych w budynku	Pracownicy/współpracownicy	Imię, nazwisko osoby uprawnionej do dostępu
16.	**Dane uczestników szkoleń PARP** Zbiór o charakterze archiwalnym.	-	Dane osobowe przetwarzane w celu wypełnienia obowiązków wynikających z przepisów prawa.	Uczestnicy szkoleń PARP.	Imię, nazwisko, adres e-mail oraz inne dane podane przez uczestników szkoleń.

17.	**Klienci (Centrum Usług)**	SAP; HDFE	Dane osobowe przetwarzane w celu realizacji zawartych z klientami umów oraz w celu wypełnienia obowiązków wynikających z przepisów prawa.	Klienci COMP S.A. Oddział Centrum Usług IT, czyli przedstawiciele, osoby reprezentujące, osoby kontaktowe, osoby fizyczne prowadzące własną działalność gospodarczą, osoby fizyczne oraz klienci końcowi – użytkownicy	Imię, nazwisko, firma, stanowisko, nr telefonu, adres e-mail, NIP, Regon, siedziba, adres prowadzenia działalności (nr domu, nr lokalu, ulica, miasto, województwo, kraj, kod pocztowy) numer rachunku bankowego, symbol banku, nazwa banku, numer faktury, kwota zobowiązania, dane klienta końcowego – użytkownika (imię, nazwisko, adres, nr tel., nr tel. komórkowy, e-mail)
18.	**Kontrahenci (Centrum Usług)**	Elektroniczny Obieg Dokumentów, SAP, system poczty e-mail	Dane osobowe przetwarzane w celu realizacji zawartych z kontrahentami umów oraz w celu wypełnienia obowiązków wynikających z przepisów prawa.	Dostawcy produktów i usług oraz inne osoby wykonujące usługi na rzecz COMP S.A., w tym: podmioty świadczące usługi serwisowe, m.in. podmioty świadczące usługi jako APS	Imię, nazwisko, firma, stanowisko, nr telefonu, adres e-mail, nr fax, NIP, PESEL, Regon, nr KRS, numer i seria dowodu osobistego, przez kogo wydany i kiedy, siedziba, adres prowadzenia działalności oraz adres zamieszkania w zakresie: nr domu, nr lokalu, ulica, miasto, województwo, kraj, kod pocztowy) numer rachunku bankowego, symbol banku, nazwa banku, numer faktury, kwota zobowiązania, Urząd Skarbowy
19.	**Lista serwisantów urządzeń komputerowych i drukujących**	HDFE, SAP, system poczty e-mail	Dane osobowe przetwarzane w celu wypełnienia obowiązków wynikających z przepisów prawa	Pracownicy COMP i podwykonawców, świadczący usługi napraw.	imię, nazwisko, PESEL, numer i seria dowodu osobistego, zdjęcie

20.	**Dane powierzone** **(Centrum Usług)**	HDFE	Dane osobowe przetwarzane w celu realizacji usług serwisowych	Osoby, których administratorem ich danych są inne podmioty - klienci COMP S.A., w szczególności klienci Centrum Usług IT na rzecz, których COMP S.A. świadczy usługi informatyczne w zakresie wdrożenia, wsparcia czy utrzymania systemów informatycznych	wszelkie kategorie danych jakie mogą się znajdować w systemach klientów
21.	**Rejestr korespondencji wychodzącej** **(Centrum Usług)**	Pocztowa książka nadawcza	Dane osobowe przetwarzane w celu obsługi klienta	Obiorcy korespondencji wychodzącej	Imię (imiona), nazwisko, firma, adres, data, przedmiot korespondencji
22.	**Rejestr przesyłek przychodzących i wychodzących** **(Centrum Usług)**	HDFE	Dane osobowe przetwarzane w celu obsługi klienta	Odbiorcy i nadawcy przesyłek urządzeń i części zamiennych	Imię (imiona), nazwisko, firma, adres, numer telefonu, data.

Załącznik nr 3 – Wzór wniosku o wydanie/cofnięcie upoważnienia

Warszawa, dnia……

……

Imię i nazwisko

……

stanowisko

……

Dział/Biuro

<u>Wniosek o wydanie/cofnięcie upoważnienia do przetwarzania danych osobowych*</u>

Zwracam się z uprzejmą prośbą o wydanie/cofnięcie upoważnienia do przetwarzania danych osobowych dla Pana/Pani……,stanowisko (ew. wskazanie na umowę cywilnoprawną)……. w związku z zawarciem/zakończeniem umowy o współpracy/zakończeniem/rozpoczęciem zatrudnienia.

……..

Data i podpis Wnioskodawcy

*niewłaściwe wykreślić

Załącznik nr 4 – Wzór oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa Danych Osobowych (dla współpracowników)

Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Danych Osobowych

Ja, ……..…… w związku z zawarciem przeze mnie ze spółką Comp S.A. umowy zlecenia/ umowy o współpracy z dn. … 20… r., niniejszym potwierdzam fakt zapoznania się z treścią Polityki Bezpieczeństwa Danych Osobowych z dnia……. .

Zobowiązuję się postępować zgodnie z zasadami ochrony danych osobowych oraz procedurami obowiązującymi w ramach tej Polityki, przy wykonywanych przeze mnie obowiązkach.

.....

Data i podpis osoby

przyjmującej zobowiązanie

Załącznik nr 5 – Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr……../……..

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO (GDPR),** niniejszym upoważniam do przetwarzania danych osobowych:

_____ (*imię, nazwisko*)

_____ (*stanowisko, ew. firma*)

w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku/ w związku z wykonywaniem czynności na podstawie umowy współpracy.

Okres ważności upoważnienia: Upoważnienie obejmuje dane osobowe, które będą przetwarzane przez upoważnionego w ramach pełnionych obowiązków służbowych na zajmowanym stanowisku/w ramach realizacji umowy o współpracy z Administratorem przez cały okres trwania zatrudnienia/ współpracy. Upoważnienie obejmuje również dane osobowe względem których Spółka COMP S.A pozostaje Procesorem.

Odbyte szkolenia: Osoba, której dotyczy upoważnienie, odbyła szkolenie wstępne z zakresu ochrony danych osobowych.

zobowiązuje się osobę upoważnioną do przetwarzania danych osobowych do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia.

…….

Podpis osoby upoważnianej

……

Administrator Danych/Pełnomocnik

Warszawa, dnia ……..

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

I. DEFINICJA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§ 1

Naruszeniem ochrony danych osobowych jest każde naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, w szczególności:

a) nieautoryzowany dostęp do danych,
b) nieautoryzowane modyfikacje lub zniszczenie danych,
c) udostępnienie danych nieautoryzowanym podmiotom,
d) nielegalne ujawnienie danych,
e) pozyskiwanie danych z nielegalnych źródeł.

II. POSTĘPOWANIE W PRZYPADKU NARUSZENIA DANYCH OSOBOWYCH

§ 2

1. Każdy pracownik lub współpracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie dokonać zgłoszenia zgodnie z SZBI (PSQ.09.7 – Zasady obsługi incydentów bezpieczeństwa) bądź równoważną polityką stosowaną w Oddziałach Spółki i filiach Oddziałów nie objętych SZBI oraz zawiadomić inspektora ochrony danych.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych, obejmują stwierdzenie następujących okoliczności:
   a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
   b) dokumentacja jest niszczona bez użycia niszczarki;
   c) fizyczna obecność w pomieszczeniach osób zachowujących się podejrzanie;
   d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.;
   e) niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, pozostawienie otwartego pomieszczenia z komputerem, zaniechanie w zakresie terminowego wykonania kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych;
   f) ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe;
   g) wynoszenie danych osobowych w wersji papierowej lub elektronicznej poza miejsce pracy bez upoważnienia;
   h) udostępnienie danych osobowych osobom nieupoważnionym;

i) modyfikacja lub próba modyfikacji, lub zmiana w strukturze danych bez odpowiedniego upoważnienia;
j) telefoniczne próby wyłudzenia danych osobowych;
k) kradzież komputerów lub twardych dysków z danymi osobowymi;
l) utrata kontroli nad kopią danych osobowych;
m) maile zachęcające do ujawnienia identyfikatora lub hasła;
n) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
o) istnienie nieautoryzowanych kont dostępu do danych;
p) przechowywanie haseł do systemów w pobliżu komputera.

§ 3

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych, zobowiązany jest natychmiastowo podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn, rozmiarów oraz skutków naruszenia.

§ 4

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych lub innej osoby upoważnionej przez administratora danych lub podmiot je przetwarzający.

§ 5

Administrator systemu informatycznego jest zobowiązany do informowania Inspektora ochrony danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6

Inspektor ochrony danych podejmuje następujące kroki:
a) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
b) odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
c) nawiązuje kontakt ze specjalistami zewnętrznymi lub służbami podmiotu powierzającego przetwarzanie danych (jeśli zachodzi taka potrzeba),
d) podejmuje decyzję w przedmiocie obowiązku zawiadomienia o naruszeniu ochrony danych osób, których dane dotyczą, jak również organu nadzorczego,
e) w razie pozytywnej weryfikacji okoliczności wskazanych w punkcie d) powyżej, dokonuje ww. zawiadomień, zgodnie z § 10.

§ 7

Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport wg wzoru stanowiącego Załącznik nr 1 niniejszej instrukcji.

§8

Inspektor ochrony danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

§ 9

Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszej instrukcji, w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych. Sankcje pracownicze nie wykluczają odpowiedzialności karnej i cywilnej, zgodnie z obowiązującymi normami prawa.

III. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

§ 10

1. W przypadku naruszenia ochrony danych osobowych, Inspektor ochrony danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Inspektor ochrony danych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze, w Rejestrze Naruszeń, zgodnie ze wzorem przyjętym w Organizacji.

IV. ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

§ 11

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Inspektor ochrony danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, z zastrzeżeniem art. 34 ust. 3 RODO.
2. Zawiadomienie, o którym mowa w ust. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33ust. 3 lit. b), c) i d) RODO.

Załącznik nr 1 do **Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych**

Raport z naruszenia ochrony danych

1. Data ……..…….. Godzina ……

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):

……

3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

……

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

……

5. Podjęte działania:

……

6. Wstępna ocena przyczyn wystąpienia naruszenia:

……

7. Postępowanie wyjaśniające i naprawcze:

……

(podpis pracownika) (data i podpis IOD)

W określonych w RODO przypadkach osoba, której dane dotyczą, ma prawo do żądania od Administratora usunięcia danych jej dotyczących. Przepis art. 17 RODO określa przesłanki, których spełnienie uprawnia do skorzystania z omawianego prawa, i przewiduje przypadki, których zaistnienie sprawia, że uprawnienie do żądania usunięcia danych nie przysługuje.

Krok 1: żądanie usunięcia danych osobowych

Jeżeli osoba, której dane dotyczą:
– stwierdzi, że dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
– cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania,
– wnosi sprzeciw wobec przetwarzania jej danych,
– stwierdzi, że dane osobowe były przetwarzane niezgodnie z prawem,
– stwierdzi, że dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega administrator,
– stwierdzi, że dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego,
to może (zgodnie z art. 17 ust. 1 RODO) zwrócić się do administratora z żądaniem usunięcia danych.
Ciężar dowodu (wykazania nieprawidłowości, nielegalności przetwarzania bądź zbędności danych) ciąży na osobie, której dane dotyczą.

Krok 2: Ocena zaistnienia jednej z przesłanek określonych w art. 17 ust. 1 RODO

Po otrzymaniu żądania usunięcia danych Administrator sprawdza, czy zachodzi jedna z przesłanek uprawniających podmiot danych do żądania usunięcia danych, określonych w art. 17 ust. 1 RODO.

a) Ocena, czy dane nie są już niezbędne do realizacji celów

Pierwszą ze wskazanych w tym przepisie przesłanek jest okoliczność, że dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane (art. 17 ust. 1 lit. a RODO).
Jeśli tak, Administrator przechodzi do Kroku 3.
Jeśli nie, Administrator przechodzi do oceny kolejnej przesłanki.

b) Ocena, czy osoba, której dane dotyczą, cofnęła zgodę

Kolejną przesłanką uprawniającą osobę, której dane dotyczą, do żądania usunięcia danych jest wycofanie zgody osoby, której dane dotyczą, na przetwarzanie danych, na której opiera się przetwarzanie danych w sytuacji, gdy nie ma innej podstawy prawnej przetwarzania danych (art. 17 ust. 1 lit. b RODO).
Jeśli tak, Administrator przechodzi do Kroku 3.
Jeśli nie, Administrator przechodzi do oceny kolejnej przesłanki.

c) Ocena, czy osoba, której dane dotyczą wniosła sprzeciw

Trzecią z przesłanek uprawniających podmiot danych do żądania usunięcia danych jest sytuacja, gdy osoba, której dane dotyczą, wniosła sprzeciw (na mocy art. 21 ust.1 RODO) wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania na cele marketingu bezpośredniego (art. 17 ust. 1 lit. c RODO).

Jeśli tak, Administrator przechodzi do Kroku 3.

Jeśli nie, Administrator przechodzi do oceny kolejnej przesłanki.

d) Ocena, czy dane osobowe były przetwarzane niezgodnie z prawem

Czwarta przesłanka uprawniająca osobę, której dane dotyczą, do żądania usunięcia danych odnosi się do sytuacji, gdy dane były przetwarzane niezgodnie z prawem, np. bez odpowiedniej podstawy prawnej (art. 17 ust. 1 lit. d RODO).

Jeśli tak, Administrator przechodzi do Kroku 3.

Jeśli nie, Administrator przechodzi do oceny kolejnej przesłanki.

e) Ocena, czy dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego

Piąta przesłanka uzasadniająca żądanie usunięcia danych dotyczy przypadków, gdy przepis prawa nakłada obowiązek usunięcia danych osobowych (art. 17 ust. 1 lit. e RODO).

Jeśli tak, Administrator przechodzi do Kroku 3.

Jeśli nie, Administrator przechodzi do oceny kolejnej przesłanki.

f) Ocena, czy dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego

Ostatnią przesłanką jest przesłanka żądania usunięcia danych w sytuacji, gdy dane zostały zebrane w związku z oferowaniem tzw. usług społeczeństwa informacyjnego, tzw. usługi internetowe (art. 17 ust. 1 lit. f RODO).

Jeśli tak, Administrator przechodzi do Kroku 3.

Jeśli nie, Administrator przekazuje wnioskodawcy informację o niespełnieniu żądania – patrz Krok 4A.

Krok 3: Wyłączenie stosowania prawa do bycia zapomnianym

W art. 17 ust. 3 RODO wskazane zostały przypadki, w których uprawnienie do żądania usunięcia danych nie ma zastosowania.

W przypadku zaistnienia choćby jednej z przesłanek określonych w kroku numer 2 niniejszej instrukcji Administrator sprawdza, czy nie zachodzi jedna ze wskazanych w art. 17 ust. 3 RODO przesłanek negatywnych – tj. przesłanek pozwalających Administratorowi na odmowę spełnienia żądania.

a) Korzystanie z prawa do wolności wypowiedzi i informacji.

Pierwszą z przesłanek jest niezbędność przetwarzania danych osobowych do korzystania z prawa do wolności wypowiedzi i informacji. W przypadku zaistnienia konfliktu pomiędzy prawem do wolności wypowiedzi i informacji, a prawem do bycia zapomnianym, przy żądaniu usunięcia danych pierwszeństwo należy się prawu do wolności wypowiedzi i informacji. Przykład: wydawca czasopisma, audycji, nie będzie

zmuszony do usunięcia danych osobowych z archiwalnego numeru czasopisma czy audycji, w którym dane zostały zgodnie z prawem opublikowane.

W przypadku stwierdzenia zaistnienia powyższej przesłanki Administrator przekazuje wnioskodawcy informację o niespełnieniu żądania – patrz Krok 4A.

b) Przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator lub wykonania zadania realizowanego w interesie publicznym bądź w ramach sprawowania władzy publicznej

Administrator weryfikuje – sprawdza obowiązujące przepisy w zakresie, w jakim wymagają one od Administratora dalszego przetwarzania. W sytuacji, gdy przepisy prawa nakładają obowiązek, do którego spełnienia konieczne jest przetwarzanie danych, Administrator odmawia spełnienia żądania osoby, której dane dotyczą, odnoszącego się do usunięcia jej danych.

W przypadku stwierdzenia zaistnienia powyższej przesłanki Administrator przekazuje wnioskodawcy informację o niespełnieniu żądania – patrz Krok 4A.

c) Ocena, czy przetwarzanie jest niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego

Przesłanką uniemożliwiającą spełnienie żądania usunięcia danych jest również szeroko rozumiany interes publiczny w dziedzinie zdrowia publicznego. W przypadku stwierdzenia zaistnienia powyższej przesłanki Administrator przekazuje wnioskodawcy informację o niespełnieniu żądania – patrz Krok 4A.

d) Ocena, czy przetwarzanie jest niezbędne do celów archiwalnych, badań naukowych, historycznych lub statystycznych

W przypadku, gdy przetwarzanie danych osobowych jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, Administrator może odmówić usunięcia danych, jednakże musi wykazać prawdopodobieństwo, że realizacja uprawnienia do usuwania danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania.

W przypadku stwierdzenia zaistnienia powyższej przesłanki Administrator przekazuje wnioskodawcy informację o niespełnieniu żądania – patrz Krok 4A.

e) Ocena, czy przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń

Ostatnią z przesłanek pozwalającą Administratorowi na odmowę spełnienia żądania usunięcia danych jest niezbędność przetwarzania do ustalenia, dochodzenia lub obrony roszczeń. Użyte w przepisie sformułowanie oznacza, że chodzi o różnego rodzaju roszczenia, rozumiane jako żądanie określonego świadczenia lub zaniechania działania.

W przypadku, gdy zaistnieje choćby jedna z przesłanek określonych w Kroku 2 i nie zaistnieje choćby jedna z przesłanek określonych w Kroku 3, Administrator **oceni, czy żądania są ewidentnie nieuzasadnione lub nadmierne.**

Administrator ocenia, czy żądanie wnioskodawcy jest ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter.

Administrator zobowiązany jest wykazać, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter.

W przypadku stwierdzenia przez Administratora, że żądanie wnioskodawcy jest ewidentnie nieuzasadnione lub nadmierne, Administrator, może:
a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działa, albo
b) odmówić podjęcia działań w związku z żądaniem.

W przypadku opłaty, Administrator wzywa wnioskodawcę do uiszczenia opłaty, wskazując jej wysokość, termin wniesienia oraz nr rachunku bankowego do jej uiszczenia. Opłata ustalana jest na zasadach określonych w art. 12 ust. 5 RODO.
Po stwierdzeniu otrzymania opłaty Administrator udziela informacji – patrz Krok 4A.

W przypadku braku uiszczenia opłaty lub w przypadku odmowy podjęcia działań Administrator przekazuje wnioskodawcy informację o niespełnieniu żądania – patrz Krok 4A.

Krok 4: spełnienie żądania

Jeżeli żądanie jest uprawnione (jest spełniona jedna z przesłanek uprawniających do żądania i nie zachodzi żadna z przesłanek negatywnych), Administrator informuje wnioskodawcę o spełnieniu żądania i usuwa kwestionowane dane.
Procedura zostaje zakończona.
W informacji o spełnieniu żądania Administrator informuje o sposobie realizacji żądania. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania - powinien udzielić osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań.
W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, to w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
Zgodnie z art. 17 ust. 2 RODO, w przypadku, gdy żądanie dotyczy danych osobowych upublicznionych przez Administratora, Administrator - biorąc pod uwagę dostępną technologię i koszt realizacji - podejmie rozsądne działania, w tym środki techniczne, by poinformować Administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych lub kopie tych danych osobowych.
Administrator informuje o usunięciu danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę o tych odbiorcach, jeśli osoba, której dane dotyczą tego zażądała.

Krok 4A: niespełnienie żądania usunięcia danych

W przypadku gdy Administrator stwierdzi, że nie zachodzi żadna z przesłanek uprawniających do żądania usunięcia danych, o których mowa w art. 17 ust. 1 RODO, lub zachodzi jedna z przesłanek wyłączających stosowanie przepisów dotyczących żądania usunięcia danych, określona w art. 17 ust. 3 RODO, to odmawia spełnienia żądania usunięcia danych.

W takiej sytuacji Administrator niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Uzyskanie informacji o spełnieniu żądania podmiotu danych kończy postępowanie w tym zakresie.

Uzyskanie informacji o niespełnieniu żądania uprawnia podmiot danych do wniesienia skargi do organu nadzorczego, zgodnie z art. 77 RODO.

Załącznik nr 8 - wzór instrukcji postępowania w przypadku zgłoszenia wniosku w przedmiocie dostępu do danych, sprostowania, modyfikacji i ograniczenia przetwarzania

---

Instrukcja określa sposób postępowania Administratora w przypadku zgłoszenia przez osobę, której dane dotyczą wniosku o udzielenie informacji, o którym mowa w art. 15 RODO.
Wszelka komunikacja związana z realizacją uprawnień określonych w niniejszym dokumencie odbywa się pisemnie lub w inny sposób, w tym w stosownych przypadkach elektronicznie. Jeżeli osoba, której dane dotyczą tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

Krok 1: wniosek o udzielenie informacji

Osoba, która chce się dowiedzieć, czy Administrator przetwarza dane na jej temat, może zwrócić się do Administratora o udzielenie informacji. Wniosek może być złożony pisemnie na adres Administratora: ul. **Jutrzenki 116** lub w formie e-mail na adres **iod@comp.com.pl** O sposobach złożenia wniosku każda osoba fizyczna, której dane są przetwarzane przez Administratora, została poinformowania zgodnie z art. 13 i art. 14 RODO. Wniosek nie wymaga uzasadnienia.

Krok 2: sprawdzenie, czy administrator przetwarza dane osobowe wnioskodawcy?

Po wpłynięciu wniosku Administrator sprawdza, czy przetwarza dane osobowe wnioskodawcy.

Stwierdzenie braku obowiązku informacyjnego.

Jeżeli Administrator nie przetwarza danych osobowych wnioskodawcy informuje o tym wnioskodawcę. W przypadku, gdy Administrator nie przetwarza danych osobowych wnioskodawcy, to nie ciąży na nim obowiązek informacyjny określony w art. 15 RODO.
W powiadomieniu o nieprzetwarzaniu Administrator informuje również wnioskodawcę, iż brak przetwarzania danych osobowych wnioskodawcy skutkuje brakiem obowiązku informacyjnego określonego w w/w przepisie.

W przypadku stwierdzenia, że dane osobowe wnioskodawcy są przetwarzane, Administrator:

Krok 3: sprawdzenie czy przepisy szczególne wyłączają obowiązek informacyjny

Administrator sprawdza istnienie obowiązku informacyjnego. Obowiązek informacyjny nie ma charakteru absolutnego i może podlegać ograniczeniom. W art. 23 RODO została przewidziana możliwość, by ustawodawca (krajowy bądź unijny) w przepisach szczególnych z ważnych powodów (np. bezpieczeństwa) ograniczył zakres praw i obowiązków (w tym również uprawnień i obowiązków informacyjnych), jeżeli zostaną spełnione przesłanki określone w tym artykule.
Mając powyższe na uwadze Administrator weryfikuje ewentualne wyłączenie obowiązku informacyjnego.

W przypadku stwierdzenia istnienia wyłączenia obowiązku informacyjnego, Administrator odmawia udzielenia wnioskodawcy informacji wskazując powody niespełnienia żądania z powołaniem na w/w przepisy wyłączające obowiązek informacyjny.
W takim przypadku procedura kończy się.

W przypadku braku przepisu szczególnego Administrator ocenia czy żądanie jest ewidentnie nieuzasadnione lub nadmierne.

Krok 4: ocena czy żądania są ewidentnie nieuzasadnione lub nadmierne

Administrator ocenia, czy żądanie wnioskodawcy jest ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter.
Administrator zobowiązany jest wykazać, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter.

W przypadku stwierdzenia przez Administratora, że żądanie wnioskodawcy jest ewidentnie nieuzasadnione lub nadmierne, Administrator, może:
a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działa, albo
b) odmówić podjęcia działań w związku z żądaniem.

W przypadku opłaty, Administrator wzywa wnioskodawcę do uiszczenia opłaty, wskazując jej wysokość, termin wniesienia oraz nr rachunku bankowego do jej uiszczenia. Opłata ustalana jest na zasadach określonych w art. 12 ust. 5 RODO.
Po stwierdzeniu otrzymania opłaty Administrator udziela informacji – patrz **KROK 5**.

W przypadku braku uiszczenia opłaty lub w przypadku odmowy podjęcia działań, Administrator informuje wnioskodawcę o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
W takim przypadku procedura kończy się.

W przypadku braku stwierdzenia przez Administratora, że żądanie jest ewidentnie nieuzasadnione lub nadmierne Administrator udziela informacji.

Krok 5: udzielenie informacji

Administrator potwierdza, że dane osobowe dotyczące osoby występującej z wnioskiem są przetwarzane przez [●], i zapewnia takiej osobie dostęp do danych oraz następujących informacji:
a) cele przetwarzania;
b) kategorie danych osobowych;

c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) informacje o prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą, wszelkie dostępne informacje o ich źródle;
h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
Ponadto, jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, Administrator informuje o odpowiednich zabezpieczeniach (o których mowa w art. 46 RODO), związanych z przekazaniem.

Ponadto Administrator informuje, że wnioskodawca ma prawo do uzyskania kopii danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się wnioskodawca, Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.

Zgodnie z art. 12 ust. 3 RODO Administrator w terminie miesiąca od otrzymania żądania udziela wnioskodawcy informacji o działaniach podjętych w związku z żądaniem lub udziela w tym terminie informacji. W razie potrzeby termin ten może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań.

Udzielenie wnioskodawcy informacji kończy procedurę.