UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta pomiędzy:

……[nazwa]……. z siedzibą w ……[adres]……., o nr NIP ……,

reprezentowaną przez: ……[osoba]……., zwaną dalej Klientem a

Comarch Spółka Akcyjna z siedzibą w Krakowie, aleja Jana Pawła II 39a, zarejestrowaną w Krajowym Rejestrze Sądowym prowadzonym przez Sąd Rejonowy dla Krakowa - Śródmieścia w Krakowie XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000057567, NIP: 677-00-65-406. Wysokość kapitału zakładowego Spółki wynosi 8.133.349,00 zł. Kapitał zakładowy został wpłacony w całości, reprezentowaną przez:

Zbigniew Rymarczyk – Wiceprezes

Michał Bajcar – Prokurent

dalej „**Comarch**".

Strony zawierają niniejszą umowę powierzenia przetwarzania danych osobowych w związku z Umową główną, na podstawie której Comarch świadczy dla Klienta w zakresie i na warunkach ustalonych w Umowie głównej usługi, które są związane z przetwarzaniem Danych Osobowych przez Comarch jako Podmiot przetwarzający.

Artykuł 1. Definicje

1.1. **Administrator** – administrator w rozumieniu art. 4 pkt 7 RODO.

1.2. **Dane osobowe** – dane osobowe w rozumieniu art. 4 pkt 1 RODO

1.3. **Dane osobowe Klienta** – Dane osobowe określone w Artykuł 2 ust. 2 Umowy powierzenia.

1.4. **Naruszenie ochrony danych osobowych** – naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO.

1.5. **Podmiot przetwarzający** – podmiot przetwarzający w rozumieniu art. 4 pkt 8 RODO.

1.6. **Przetwarzanie** – przetwarzanie danych osobowych w rozumieniu art. 4 pkt 2 RODO.

1.7. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady(UE) 2016/679 z dnia 27 kwietnia 2016r. 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).

1.8. **Umowa główna** – umowa na świadczenie Usługi Comarch OCR&KSeF zgodnie z Regulaminem Usługi Comarch OCR&KSeF

1.9. **Umowa powierzenia** – niniejsza umowa powierzenia przetwarzania danych osobowych, stanowiąca zgodnie z wolą Stron integralną część Umowy głównej.

Artykuł 2. Przedmiot umowy

2.1. Niniejsza Umowa określa warunki Przetwarzania przez Comarch w imieniu Administratora Danych osobowych Klienta określonych poniżej w Artykuł 2 ust. 2 w zakresie Usług wykonywanych na podstawie Umowy głównej.

2.2. Klient powierza Comarch Przetwarzanie następujących Danych osobowych:

2.2.1. Rodzaj danych osobowych objętych Umową:

- dane identyfikacyjne (imię, nazwisko, adres e-mail, login, nr telefonu)
- dane adresowe (kod, kraj, miasto, ulica, numer domu)
- pozostałe dane załączone w skanach dokumentów przekazanych do usługi (np. zamówienia u dostawców, oferty sprzedaży, faktury proforma, faktury sprzedaży, faktury zaliczkowe, paragony, faktury zakupu, korekty faktur)
- historia komunikacji

- historia logowania

W przypadku konieczności dodania dodatkowego rodzaju danych osobowych niewskazanych na liście powyżej, Klient poinformuje o tym Comarch w formie pisemnej, przy czym każdorazowa modyfikacja danych osobowych wskazanych na liście nie wymaga formy aneksu do niniejszej Umowy, a jedynie pisemnego oświadczenia Klienta złożonego Comarch z dokładnym wskazaniem rodzaju danych osobowych, jakie dodatkowo są wprowadzane.

2.2.2. Kategorie osób, których Dane osobowe dotyczą:

- użytkownicy usługi Comarch OCR&KSeF świadczonej na podstawie Regulaminu świadczenia usług Comarch OCR&KSeF
- osoby fizyczne
- osoby prawne

2.3. Comarch będzie przetwarzał Dane osobowe Klienta w zakresie usług wykonywanych na podstawie Umowy głównej.

2.4. Powierzenie Przetwarzania Danych osobowych Klienta następuje w celu wykonania Umowy głównej.

Artykuł 3. Przetwarzanie Danych osobowych Klienta przez Comarch

3.1. Comarch będzie przetwarzał Dane Osobowe Klienta wyłącznie w celu, w zakresie i na warunkach określonych w Umowie powierzenia.

3.2. Comarch będzie przetwarzał Dane osobowe Klienta w zakresie świadczenia Usług wyłącznie w formie elektronicznej w systemie informatycznym.

3.3. Strony uzgadniają, że Dane osobowe Klienta będą przetwarzane zgodnie z poleceniami Administratora, które powinny być przesyłane do Comarch przez Klienta w formie pisemnej. Polecenia przekazane w innej formie nie są wiążące do momentu ich przesłania w uzgodnionej formie. Termin realizacji każdego polecenia powinien być uzgodniony przez Strony. Polecenie, które dotyczy zmiany zakresu lub sposobu świadczenia Usług lub wykonania dodatkowej usługi jest traktowane jak zlecenie Comarch dodatkowej usługi, za wykonanie której Comarch może zażądać dodatkowego wynagrodzenia. Takie polecenie może zostać złożone wyłącznie na warunkach określonych w Umowie głównej dla zamawiania dodatkowych usług lub, jeżeli Umowa główna nie reguluje zasad zamawiania dodatkowych usług, poprzez podpisanie przez obie Strony odpowiedniego zamówienia lub aneksu do Umowy głównej i za wynagrodzeniem obliczonym według stawek określonych w Umowie głównej lub, w razie braku takich stawek w Umowie głównej, według aktualnego cennika Comarch. Do polecenia, które dotyczy środków technicznych i organizacyjnych stosowanych przez Comarch zastosowanie ma Artykuł 6 ust.4.

3.4. Comarch poinformuje Klienta, jeżeli polecenie Administratora przekazane mu zgodnie z Artykuł 3 ust.3, uznać należy za niezgodne z RODO lub innymi przepisami o ochronie danych osobowych.

Artykuł 4. Okres przetwarzania

4.1. Dane osobowe Klienta będą przetwarzane przez Comarch w okresie wykonywania Usług, z zastrzeżeniem Artykuł 4 ust. 2 i 3.

4.2. O ile Umowa główna nie stanowi inaczej, po zakończeniu współpracy Stron na podstawie Umowy głównej, Comarch wyda Klientowi Dane osobowe Klienta, które na dzień przekazania będą znajdowały się w posiadaniu Comarch, zgodnie z warunkami i w terminie określonym w Umowie głównej. Jeżeli Umowa główna nie określa warunków lub terminu wydania Danych osobowych Klienta, wydanie tych danych następuje na podstawie zamówienia Klienta za dodatkowym wynagrodzeniem według stawek określonych w Umowie głównej lub, w razie braku takich stawek w Umowie głównej, według aktualnego cennika Comarch.

4.3. O ile Umowa główna nie stanowi inaczej, Comarch usuwa Dane osobowe Klienta oraz ich kopie niezwłocznie po upływie okresu niezbędnego do ustalenia, dochodzenia lub obrony roszczeń wynikających lub mogących wynikać z Umowy głównej lub Umowy powierzenia.

4.4. Postanowienia Artykuł 4 ust. 2 i 3 pozostają w mocy po rozwiązaniu lub wygaśnięciu Umowy powierzenia.

Artykuł 5. Obowiązki Comarch

5.1. Comarch zobowiązuje do przestrzegania Umowy powierzenia i właściwych przepisów prawa mających zastosowanie do Przetwarzania Danych osobowych stanowiącego przedmiot Umowy powierzenia, w szczególności zobowiązuje się do przestrzegania obowiązków Podmiotu przetwarzającego wynikających z RODO.

5.2. Comarch zapewnia, by osoby upoważnione przez Comarch do Przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.

5.3. Comarch podejmuje środki organizacyjne i techniczne właściwe zgodnie z art. 32 RODO do Przetwarzania Danych osobowych Klienta przez Podmiot przetwarzający w zakresie Usług świadczonych zgodnie z Umową główną. Opis standardowych środków organizacyjnych i technicznych stosowanych przez Comarch określa Załącznik „Standardowe środki techniczne i organizacyjne". Comarch jest uprawniony do dokonania wyboru lub zmiany tych środków organizacyjnych i technicznych, o ile nie spowoduje to naruszenia warunków Umowy głównej. Strony mogą uzgodnić w opisie Usług w Umowie głównej dodatkowe środki organizacyjne i techniczne, które powinien wdrożyć Comarch. Klient może zlecić Comarch zmianę lub wdrożenie dodatkowych środków organizacyjnych i technicznych zgodnie z Artykułem 6 ust.4.

5.4. W zakresie pomocy dla Administratora przy realizacji obowiązku wdrożenia przez Administratora odpowiednich środków organizacyjnych i technicznych, o której mowa art.28 ust. 3 pkt f) RODO, uwzględniając charakter Przetwarzania oraz dostępne mu informacje, Comarch zobowiązany jest do :

5.4.1. wdrożenia w Comarch środków organizacyjnych i technicznych zgodnie z Artykuł 5 ust.3;

5.4.2. udzielania w miarę możliwości informacji o możliwych do zastosowania innych lub dodatkowych środkach technicznych i organizacyjnych - na zapytanie Klienta złożone na podstawie Artykuł 6 ust.1;

5.5. W zakresie pomocy dla Administratora przy realizacji obowiązku wykonania oceny skutków dla ochrony danych oraz uprzednich konsultacji z organem nadzorczym, o której mowa art.28 ust. 3 pkt f) RODO, uwzględniając charakter Przetwarzania oraz dostępne mu informacje, Comarch zobowiązany jest do:

5.5.1. udostępnienia na żądanie Administratora standardowej dokumentacji Comarch zawierającej opis środków technicznych i organizacyjnych stosowanych przez Comarch zgodnie z Artykuł 5 ust.3;

5.5.2. udzielania w miarę możliwości dodatkowych informacji dotyczących stosowanych lub możliwych do zastosowania przez Comarch środków technicznych i organizacyjnych - na zapytanie Klienta złożone na podstawie Artykuł 6 ust.1;

5.5.3. udzielania w miarę możliwości dodatkowych informacji związanych z zapytaniem organu nadzorczego w toku uprzednich konsultacji - na zapytanie Klienta złożone na podstawie Artykuł 6 ust.1;

5.6. W zakresie pomocy dla Administratora przy realizacji obowiązku dokonywania zgłoszenia Naruszenia ochrony danych osobowych do organu nadzorczego oraz zawiadamiania o Naruszeniu ochrony danych osobowych osób, których dane dotyczą, o której mowa art.28 ust. 3 pkt f) RODO, uwzględniając charakter Przetwarzania oraz dostępne mu informacje Comarch zobowiązany jest do:

5.6.1. zgłoszenia Klientowi bez zbędnej zwłoki na adres email wskazanym przez Klienta do korespondencji z tematem poprzedzonym oznaczeniem [RODO] Naruszenia ochrony danych osobowych stwierdzonego przez Comarch w związku z wykonywaniem Umowy powierzenia;

5.6.2. udzielenia Klientowi w miarę możliwości dodatkowych informacji dotyczących stwierdzonego przez Klienta lub zgłoszonego przez Comarch Naruszenia ochrony danych osobowych w zakresie niezbędnym do ustalenia przez Klienta prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności osób, których Dane osobowe są objęte tym naruszeniem, oraz w zakresie niezbędnym do dokonania przez Klienta zgodnie z art. 33 i 34 RODO zgłoszenia Naruszenia ochrony danych osobowych do organu nadzorczego lub zawiadamiania o Naruszeniu ochrony danych osobowych osób, których dane dotyczą - na zapytanie Klienta złożone na podstawie Artykuł 6 ust.2.

5.7. W przypadku stwierdzenia Naruszenia ochrony danych osobowych spowodowanego z winy Comarch lub z winy podwykonawcy Comarch, Comarch dokona przeglądu stosowanych środków technicznych i organizacyjnych oraz w razie potrzeby i w miarę możliwości wprowadzi odpowiednie zmiany w celu zapobiegnięcia powtórzeniu się takiego Naruszenia ochrony danych osobowych w przyszłości.

Artykuł 6. Uprawnienia Klienta

6.1. W okresie obowiązywania Umowy głównej Klient jest uprawniony do składania zapytań o informacje określonych w Artykuł 5 oraz żądania - w stopniu nieprzekraczającym racjonalnych granic tych aktywności, od Comarch udzielenia informacji dotyczących sposobu wykonywania Umowy powierzenia przez Comarch. W tym zakresie Klient może kierować zapytania przez System Obsługi Zgłoszeń (www.asysta.comarch.pl). Realizacja zapytań Klienta może polegać na odpowiedzi na pojedyncze pytania, na przygotowaniu ustalonych przez Strony raportów lub analiz lub innej ustalonej przez Strony formie odpowiedzi - w stopniu nieprzekraczającym racjonalnych granic tych aktywności i jest wykonywana w ramach wynagrodzenia za świadczenie Usług, o którym mowa w Umowie głównej.

6.2. Klient jest uprawniony do składania zapytań o informacje dotyczące Naruszenia ochrony danych osobowych, o którym mowa w Artykuł 5 ust.6 w drodze korespondencji pisemnej. Realizacja zapytań Klienta może polegać na odpowiedzi na pojedyncze pytania lub mieć inną ustaloną przez Strony formę i jest wykonywana w ramach wynagrodzenia za świadczenie Usług, o którym mowa w Umowie główne, jeżeli Naruszenie ochrony danych osobowych zostało spowodowane z winy Comarch. W innych przypadkach do zapytań Klienta, o których mowa w Artykuł 5 ust.6, stosuje się Artykuł 6 ust. 1.

6.3. Klient jest upoważniony do przeprowadzenia audytu w celu weryfikacji przestrzegania Umowy powierzenia przez Comarch, bezpośrednio lub za pośrednictwem upoważnionego audytora, z zastrzeżeniem następujących warunków:

6.3.1. audytorem Klienta nie może być podmiot prowadzący działalność konkurencyjną wobec Comarch S.A. lub innej spółki z grupy Comarch, ani podmiot z nim powiązany lub jego pracownik lub podmiot/osoba z nim współpracująca, bez względu na podstawę zatrudnienia lub współpracy;

6.3.2. audyt może obejmować wysyłanie zapytań, analizę dokumentów, rozmowy z pracownikami/współpracownikami Comarch lub podwykonawców Comarch oraz wizytację lokali Comarch lub podwykonawców Comarch, o ile mają bezpośredni związek w wykonywaniem Umowy powierzenia;

6.3.3. audyt nie może obejmować informacji lub dokumentów dotyczących innych klientów Comarch, ani zmierzać lub skutkować uzyskaniem dostępu Klienta do Danych Osobowych innych niż Dane Osobowe Klienta lub do danych poufnych Comarch lub innych podmiotów;

6.3.4. Comarch może uzależnić udział audytora lub wyznaczonego pracownika Klienta w audycie od uprzedniego zawarcia odpowiedniej umowy poufności z Comarch lub podwykonawcą Comarch;

6.3.5. w czasie audytu Klient i audytor mają obowiązek przestrzegania wewnętrznych procedur i polityk Comarch lub podwykonawcy Comarch dotyczących bezpieczeństwa i poufności;

6.3.6. audyt nie powinien być przeprowadzany częściej niż raz w roku kalendarzowym i nie powinien trwać dłużej niż 14 dni;

6.3.7. termin audytu powinien być uzgodniony przez Strony, przy czym Klient powinien zgłosić zamiar przeprowadzenia audytu co najmniej 30 dni przed jego proponowanym terminem, wysyłając zgłoszenie przez System Obsługi Zgłoszeń (www.asysta.comarch.pl);

6.3.8. Comarch zobowiązany jest do aktywnego udziału w audycie i odpowiedniej współpracy z Klientem i audytorem;

6.3.9. każda ze Stron pokrywa własne koszty związane z przeprowadzeniem audytu, przy czym Klient pokrywa każdorazowo wszystkie koszty audytora.

6.4. Klient może w każdym czasie wnioskować o wdrożenie nowych lub zmianę stosowanych przez Comarch środków technicznych i organizacyjnych, o których mowa w Artykuł 5 ust. 3. W przypadku takiego żądania Klienta, o ile jest to zasadne i możliwe do zrealizowania bez zmiany organizacji lub naruszenia ciągłości działania przedsiębiorstwa Comarch lub jego podwykonawcy, Comarch przedłoży Klientowi ofertę i Strony ustalą w drodze negocjacji warunki zmiany lub wdrożenia nowych środków technicznych i organizacyjnych.

6.5. Klient powinien korzystać z uprawnień określonych w niniejszej Umowie powierzenia w taki sposób by nie zakłócić wykonywania Umowy głównej oraz prowadzenia bieżącej działalności przez Comarch i jego podwykonawców.

Artykuł 7. Oświadczenia i obowiązki Klienta

7.1. Klient oświadcza, że jest Administratorem Danych osobowych Klienta i gwarantuje, że są przez niego przetwarzane zgodnie z prawem.

7.2. Klient oświadcza, że zapoznał się z Załącznikiem „Standardowe środki techniczne i organizacyjne" przed podpisaniem niniejszej Umowy powierzenia i akceptuje go bez zastrzeżeń.

7.3. Klient oświadcza, że dokonał wyboru Comarch jako usługodawcy, biorąc pod uwagę wiedzę fachową, wiarygodność i zasoby Comarch oraz jego ofertę w zakresie zapewnienia wdrożenia odpowiednich środków technicznych i organizacyjnych.

7.4. Klient zobowiązuje do przestrzegania Umowy powierzenia oraz właściwych przepisów prawa mających zastosowanie do Przetwarzania danych osobowych, w szczególności zobowiązuje się do przestrzegania obowiązków Administratora wynikających z RODO.

Artykuł 8. Podwykonawcy Comarch

8.1. Klient wyraża niniejszym zgodę na dalsze powierzenie Przetwarzania Danych osobowych Klienta w ramach usług zlecanych przez Comarch następującym podwykonawcom:

- iComarch24 S.A. z siedzibą w Krakowie, nr KRS: 0000328672, NIP: 6751410687 w celu realizacji funkcjonalności integracji z systemami wytwarzanymi przez iComarch24 S.A
- Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA

8.2. Klient wyraża zgodę na dalsze powierzenie Przetwarzania Danych osobowych Klienta w ramach usług zlecanych przez Comarch innym podmiotom po uprzednim powiadomieniu Klienta o takim podwykonawcy z co najmniej 7-dniowym wyprzedzeniem poprzez komunikat na stronie www.erpxt.pl

8.3. Comarch zobowiązuje się współpracować z takimi podwykonawcami, którzy zapewniają wdrożenie takich środków technicznych i organizacyjnych, aby Przetwarzanie odpowiadało wymogom RODO.

8.4. Comarch zawrze z każdym podwykonawcą, który będzie przetwarzał Dane osobowe Klienta stosowną umowę, nakładającą na podwykonawcę odpowiednie obowiązki ochrony Danych osobowych.

8.5. Jeżeli podwykonawca Comarch nie wywiąże się ze spoczywających na nim obowiązków ochrony Danych osobowych Klienta, Comarch ponosi wobec Klienta odpowiedzialność za niewypełnienie obowiązków przez podwykonawcę tak jak za własne działania i zaniechania.

Artykuł 9. Odpowiedzialność Stron Umowy

9.1. Klient odpowiada za prawidłowe wykonywanie obowiązków Administratora zgodnie z RODO, innymi właściwymi przepisami ochrony danych osobowych i niniejszą Umową powierzenia.

9.2. Comarch odpowiada za prawidłowe wykonywanie obowiązków Podmiotu przetwarzającego zgodnie z RODO, innymi właściwymi przepisami ochrony danych osobowych i niniejszą Umową powierzenia.

9.3. Umowa powierzenia stanowi integralną część Umowy głównej i jej naruszenie stanowi naruszenie Umowy głównej. W związku z tym, w zakresie dozwolonym przepisami prawa, odpowiedzialność każdej ze Stron wobec

drugiej Strony Umowy powierzenia, z tytułu naruszenia RODO, innych właściwych przepisów ochrony danych osobowych lub Umowy powierzenia podlega ograniczeniu lub wyłączeniu zgodnie z postanowieniami Umowy głównej.

9.4. Odpowiedzialność Comarch za wykonanie polecenia Administratora, które jest niezgodne z RODO lub innymi przepisami o ochronie danych osobowych oraz w związku z poleceniami Administratora, które nie zostały złożone zgodnie z Artykuł 3 ust.3, jest wyłączona.

9.5. Postanowienia Artykuł 9 pozostają w mocy po rozwiązaniu lub wygaśnięciu Umowy powierzenia.

Artykuł 10. Wyłączna właściwość sądu i wybór prawa właściwego dla Umowy

10.1. Strony uzgadniają, że właściwe dla Umowy powierzenia będzie prawo obowiązujące w Polsce, zaś do rozstrzygania sporów właściwy będzie sąd powszechny w Krakowie.

10.2. W sprawach nieuregulowanych w niniejszej Umowie powierzenia zastosowanie będzie miało RODO oraz właściwe przepisy prawa polskiego

Artykuł 11. Postanowienia końcowe

11.1. Umowa powierzenia wchodzi w życie ze skutkiem od dnia wejścia w życie Umowy głównej, stanowi integralną część Umowy głównej i zostaje zawarta na okres wykonywania Umowy głównej.

11.2. Rozwiązanie lub wygaśniecie Umowy głównej skutkuje odpowiednio rozwiązaniem lub wygaśnięciem Umowy powierzenia bez potrzeby składania dodatkowych oświadczeń. Rozwiązanie Umowy powierzenia przed upływem okresu na jaki została zawarta Umowa główna bez jednoczesnego rozwiązania Umowy głównej jest wyłączone.

11.3. Przeniesienie praw i obowiązków wynikających z niniejszej Umowy powierzenia jest dopuszczalne wyłącznie w przypadku, gdy następuje przeniesienie praw i obowiązków wynikających z Umowy głównej. W takim wypadku zmiana Strony Umowy powierzenia następuje na takich samych warunkach jakie określa Umowa główna dla zmiany Strony Umowy głównej.

11.4. Strony uzgadniają, że Przetwarzanie danych osobowych będzie wykonywane wyłącznie na terytorium Unii Europejskiej. Przekazanie przez Comarch Danych osobowych Klienta do państwa trzeciego wymaga uprzedniej zgody Klienta w formie pisemnej lub dokumentowej, chyba że obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem Przetwarzania Comarch informuje Klienta o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

11.5. Umowa powierzenia i Umowa główna regulują w sposób całkowity uzgodnione przez Strony warunki Przetwarzania Danych osobowych Klienta przez Comarch w związku z wykonywaniem Usług i uchylają jakiekolwiek wcześniejsze ustalenia Stron dokonane w tym zakresie. W przypadku rozbieżności postanowień Umowy powierzenia i Umowy głównej pierwszeństwo mają postanowienia Umowy powierzenia.

11.6. Integralną część Umowy powierzenia stanowi Załącznik „Standardowe środki techniczne i organizacyjne".

11.7. Umowa powierzenia została podpisana w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

11.8. Dane są przetwarzane na terenie UE.

Załącznik - Standardowe środki techniczne i organizacyjne

Niniejszy załącznik przedstawia ogólny opis standardowych środków technicznych i organizacyjnych stosowanych przy świadczeniu dla klientów usług związanych z przetwarzaniem danych osobowych. Umowa główna może określać dodatkowe lub inne środki techniczne i organizacyjne uzgodnione przez Strony i w tym zakresie postanowienia Umowy głównej będą miały pierwszeństwo przed postanowieniami niniejszego załącznika.

I. Środki organizacyjne - Procedury i polityki obowiązujące w grupie Comarch

1. W spółkach z grupy Comarch wdrażane są niezbędne procedury i polityki służące m.in. zapewnieniu bezpieczeństwa, poufności, integralności i dostępności danych klientów (w tym danych osobowych, w stosunku do których administratorami są klienci), do których w ramach świadczonych usług uzyskują dostęp pracownicy lub współpracownicy spółek z grupy Comarch.
2. Spółka Comarch S.A. posiada certyfikat ISO 27001 i wdrożyła procedury i powiązane z nimi instrukcje określające w szczególności:
   a) Politykę bezpieczeństwa
   b) Politykę zarządzania siecią informatyczną Comarch
   c) Zasady administracji systemami i aplikacjami
   d) Zasady przebywania na terenie Comarch i dostępu do pomieszczeń Comarch
   e) Zasady użytkowania aktywów i wynoszenie sprzętu
   f) Zasady zabezpieczenia komputerów osobistych
   g) Zasady korzystania z nośników informacji
   h) Zasady dostępu zdalnego
   i) Zasady bezpieczeństwa poczty elektronicznej
   j) Politykę haseł
   k) Politykę ciągłości działania
   l) Politykę antywirusową
3. W pozostałych spółkach z grupy Comarch wdraża się niezbędne procedury i polityki co do zasady oparte na procedurach obowiązujących w głównej spółce w grupie, w zakresie uwzględniającym specyfikę i działalność tych spółek.
4. Wdrażane są ponadto dedykowane procedury służące zapewnieniu prawidłowego wykonania wynikających z RODO obowiązków spółek Comarch jako administratorów oraz obowiązków spółek Comarch jako podmiotów przetwarzających (w stosunku do danych klientów).
5. Spółki z grupy Comarch współpracują w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych, zapewniając tym samym odpowiedni standard bezpieczeństwa dla klientów grupy Comarch.

II. Środki techniczne i organizacyjne – kontrola dostępu

1. W spółkach z grupy Comarch wdrażane są odpowiednie środki techniczne i organizacyjne zapewniające ograniczenie dostępu do budynków, systemów, środowisk i zbiorów danych wyłącznie dla osób upoważnionych.
2. W budynkach Comarch wydzielane są strefy publicznie dostępne oraz strefy z dostępem zastrzeżonym dla osób upoważnionych.
3. Pracownicy lub współpracownicy korzystają z kart dostępowych lub stosowane są inne metody kontroli fizycznego dostępu do nieruchomości, budynków lub pomieszczeń Comarch, zapewniające kontrolę dostępu poszczególnych osób odpowiednią do zakresu ich uprawnień.
4. Nadawanie uprawnień poszczególnym pracownikom lub współpracownikom w zakresie dostępu do systemów wewnętrznych Comarch oraz środowisk klienta podlega procedurze umożliwiającej kilkustopniową weryfikację wniosku o nadanie uprawnień.
5. Dostęp do systemów wewnętrznych i środowisk oraz danych klientów możliwy jest tylko dla upoważnionych pracowników lub współpracowników po zalogowaniu na indywidualne konto i przy użyciu indywidualnego hasła zgodnego z Polityką haseł.
6. Zdalny dostęp pracowników lub współpracowników do sieci grupy Comarch i późniejsza wymiana informacji odbywają się po uwierzytelnieniu przy wykorzystaniu bezpiecznych mechanizmów, zapewniających poufność i integralność (np. VPN IPSec).
7. W celu zapewnienia bezpieczeństwa, tam gdzie jest to uzasadnione oraz zgodne z prawem, Comarch stosuje monitoring i współpracuje z firmami ochroniarskimi.

III. Środki techniczne i organizacyjne – Comarch Data Center

1. Comarch oferuje klientom korzystanie z Comarch Data Center, tj. data center zarządzanych przez jedną ze spółek z grupy Comarch.
2. Comarch Data Center bazuje na praktykach ITIL v3. w zakresie następujących procesów: zarządzanie zmianą (change management), zarządzanie incydentem (incident management), zarządzanie problemem (problem management), service level management oraz zarządzanie konfiguracją (configuration management). Ponadto, wdrożone są odpowiednie procesy w zakresie: zarządzania aktualizacjami i łatkami (patch management), zarządzanie ryzykiem, procedury backupowe i odtworzeniowe, zarządzanie ciągłością biznesu (business continuity management), raportowania, DRP, przeglądów logów oraz przeglądy dostępów i uprawnień.
3. Backup systemów wewnętrznych podlega centralnemu systemowi backupów zgodnie z Procedurą Backup serwerów.
4. Backup systemów klientów oraz backup danych klientów podlegają zasadom określonym w umowach z klientami. Standardowe procedury Comarch Data Center przewidują maksymalny okres retencji backupów

do 3 miesięcy), przy czym okres retencji może zostać wydłużony na żądanie klienta zgodnie z postanowieniami Umowy Głównej.

5. Wstęp do Comarch Data Center mają jedynie inżynierowie Comarch Data Center oraz działy bezpieczeństwa. Inne osoby mogą przebywać na terenie Comarch Data Center tylko w uzasadnionych przypadkach oraz wyłącznie w obecności przedstawiciela Comarch. Dostęp do poszczególnych pomieszczeń na terenie Comarch Data Center może podlegać dalszym ograniczeniom.
6. Stosowana jest logiczna bądź fizyczna separacja środowisk poszczególnych Klientów (VLANy, VMy itp.)
7. Do poszczególnych środowisk mają dostęp jedynie pracownicy lub współpracownicy odpowiedzialni za obsługę poszczególnych klientów i ich działania na systemach klientów są logowane.
8. Wymogowi „segregation of duties" podlegają również inżynierowie Comarch Data Center. W związku z tym, tworzone są dedykowane zespoły dla:
   a) systemów Linux/Unix,
   b) systemów Windows,
   c) baz danych,
   d) systemów FireWall (wewnętrznych) oraz Load Balancerów.
   e) infrastruktury sieciowej w Data Center oraz FireWalli zewnętrznych
9. Każdy ośrodek Data Center wyposażony jest w dwie linie klastrów systemów FireWall od dwóch czołowych, niezależnych producentów.
   a) Klaster zewnętrzny chroniący dostępu do DMZ,
   b) Klaster wewnętrzny kontrolujący przepływy danych pomiędzy DMZ a strefą Bazodanową.
10. W Comarch Data Center stosuje się kilka niezależnych łączy internetowych dywersyfikując media (np. miedź, światło, radio, uruchomiony protokół BGP).
11. Komunikacja pomiędzy siecią Klienta a Comarch Data Center jest szyfrowana (np. IPSec, SSL VPN).
12. Comarch Data Center stosuje:
   a) niezależne i redundantne obiegi klimatyzacji z jednym aktywnym obiegiem;
   b) redundantne linie energetycznie z jedną aktywną ścieżką;
   c) systemy zasilania awaryjnego (UPS'y lub generatory prądotwórcze);
   d) wielostrefową ochronę przeciwpożarową;
   e) system gaśniczy oparty o gaz neutralny lub gaz chemiczny;
   f) alarm przeciwpożarowy oraz automatyczna notyfikacja.
13. W przypadku decyzji Klienta o wyborze innego data center, stosowane środki techniczne i organizacyjne określa wybrany dostawca usług. W przypadku, gdy Comarch korzysta z podwykonawcy w zakresie świadczenia usług hostingowych dla Klienta, podwykonawca zobowiązany jest do wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO oraz Umowy powierzenia zawartej przez Comarch z Klientem.

IV. Zarządzanie incydentami bezpieczeństwa

W Comarch wdrożono procedurę zarządzania incydentami naruszenia bezpieczeństwa i nałożono na wszystkich pracowników obowiązek zgłaszania wszelkiego rodzaju incydentów naruszenia bezpieczeństwa, w tym incydentów dotyczących naruszenia ochrony danych osobowych.

V. Szkolenia i audyty

1. W Comarch wdrożono procedurę zapewniającą okresowe szkolenia pracowników z zakresu obowiązującej polityki i procedur bezpieczeństwa oraz przepisów i procedur dotyczących ochrony danych osobowych.
2. Audyty bezpieczeństwa systemów wewnętrznych grupy Comarch przeprowadzane są okresowo przez Dział Bezpieczeństwa Wewnętrznego Comarch S.A.
3. Comarch S.A. okresowo przechodzi audyty realizowane przez jednostki certyfikujące.
4. Audyty systemów klientów podlegają zasadom określonym w umowach z klientami. Comarch współpracuje z klientami w zakresie kontroli i audytów przeprowadzanych przez klientów lub wyznaczonych audytorów zewnętrznych w zakresie uzgodnionym przez strony w umowie, przy zachowaniu procedur bezpieczeństwa obowiązujących w grupie Comarch oraz przy uwzględnieniu tajemnicy przedsiębiorstwa oraz obowiązku zachowania w poufności danych i warunków współpracy z innymi klientami.