POLITYKA
OCHRONY DANYCH OSOBOWYCH

1. DEFINICJE

1.1. **Administrator** (także **Spółka** lub **Organizacja**) – dana spółka z grupy CRH w Polsce.

1.2. **Dane osobowe** lub **dane** - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

1.3. **Zespół IT** – oznacza Pracowników odpowiedzialnych za nadzorowanie i koordynację pracy Systemów Informatycznych, z których korzysta Spółka, oraz za zapewnienie bezpieczeństwa Systemów Informatycznych;

1.4. **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

1.5. **Szczególne kategorie Danych osobowych** - Dane osobowe zawierające następujące informacje dotyczące osoby fizycznej: pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania filozoficzne, członkostwo w związkach zawodowych, dane genetyczne, biometryczne (np. odciski palców lub obrazy twarzy), dane dotyczące zdrowia, życia seksualnego lub orientacji seksualnej oraz wszelkie dane osobowe dotyczące wyroków skazujących za przestępstwa lub wykroczenia.

1.6. **Osoba upoważniona do przetwarzania danych osobowych** - osoba posiadająca upoważnienie do przetwarzania danych osobowych.

1.7. **Koordynator ds. ochrony danych osobowych (KODO)** – osoba wskazana przez Administratora wspierająca go w zakresie koordynowania wykonywania zadań związanych z zapewnieniem zgodności przetwarzania danych osobowych w Spółce z obowiązującym prawem.

1.8. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

1.9. **Naruszenie ochrony danych osobowych** - 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.

1.10. **Organ nadzorczy** – PUODO lub inny właściwy organ nadzorczy dla spraw z zakresu ochrony Danych osobowych wyznaczony przez inne państwo członkowie Unii Europejskiej lub Unię Europejską.

1.11. **Polityka** – niniejsza Polityka ochrony danych.

1.12. **Podmiot danych** – osoba fizyczna, której dotyczą Dane osobowe przetwarzane przez Administratora.

1.13. **Podmiot przetwarzający dane** - podmiot, który przetwarza Dane osobowe w imieniu Administratora.

1.14. **Pracownik** – osoba fizyczna zatrudniona przez Administratora na podstawie umowy o pracę lub innej umowy cywilnoprawnej (np. umowa zlecenie, umowa o dzieło).

1.15. **PUODO** – Prezes Urzędu Ochrony Danych Osobowych.

1.16. **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.

1.17. **EOG** – Europejski obszar Gospodarczy,

1.18. **Państwo trzecie** – państwo nienależące do EOG,

1.19. **Transgraniczne przetwarzanie** – przetwarzanie obejmujące:

1.19.1. przetwarzanie Danych osobowych, które odbywa się w Unii Europejskiej w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim Administratora lub Podmiotu przetwarzającego w Unii Europejskiej posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo

1.19.2. przetwarzanie Danych osobowych, które odbywa się w Unii Europejskiej w ramach działalności pojedynczej jednostki organizacyjnej Administratora lub Podmiotu przetwarzającego w Unii Europejskiej, ale które znacznie wpływa lub może znacznie wpłynąć na Podmioty danych, w więcej niż jednym państwie członkowskim.

1.20. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

2. ZASADY OGÓLNE

2.1. Niniejsza Polityka stanowi podstawowy dokument regulujący zasady Przetwarzania danych przez Administratora. Dodatkowo Polityka przedstawia obowiązki i odpowiedzialność Spółki w zakresie ochrony Danych osobowych.

2.2. Spółka przetwarza Dane osobowe:

2.2.1. zgodnie z prawem, rzetelnie i w sposób przejrzysty dla Podmiotu danych;

2.2.2. w konkretnych, wyraźnych i prawnie uzasadnionych celach i przetwarza je tylko w sposób zgodny z tymi celami;

2.2.3. w sposób adekwatny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane;

2.2.4. prawidłowe i w razie potrzeby uaktualniane, podejmując wszelkie rozsądne działania, aby Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

2.2.5. w formie umożliwiającej identyfikację Podmiotu danych, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;

2.2.6. w sposób zapewniający odpowiednie bezpieczeństwo Danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

2.3. Administrator podejmuje stałe działania mające na celu zapewnienie legalności przetwarzania i doskonalenie bezpieczeństwa przetwarzanych Danych osobowych będących w jego posiadaniu i powierzonych mu do przetwarzania przez inne podmioty na podstawie umów.

2.4. Administrator zapewnia przestrzeganie Polityki przez wszystkich Pracowników. Administrator zapoznaje swoich Pracowników z zasadami ochrony Danych osobowych, w szczególności z niniejszą Polityką oraz przeprowadza cykliczne szkolenia z tego zakresu, w tym szkolenia on-line.

2.5. W przypadku współpracy z podmiotem trzecim obejmującej przetwarzanie Danych osobowych na zlecenie Administratora (Podmiotem przetwarzającym dane), Spółka zapewnia, by została zawarta z takim podmiotem umowa powierzenia przetwarzania Danych osobowych oraz aby taki podmiot trzeci zobowiązał się do zapewnienia odpowiedniego poziomu ochrony Danych osobowych, z uwzględnieniem postanowień Polityki.

2.6. W przypadku współpracy z podmiotem trzecim, obejmującej przetwarzanie przez Administratora Danych osobowych na zlecenie tego podmiotu, Spółka zawiera umowę powierzenia przetwarzania Danych osobowych oraz zapewnia stosowanie się do jej wymogów przez wszystkie osoby zaangażowane w tę współpracę.

2.7. Administrator poprzez odpowiednie środki techniczne i organizacyjne zapewnia możliwość wykazania zgodności przetwarzania Danych osobowych z RODO oraz pozostałymi przepisami dotyczącymi ochrony Danych osobowych („zasada rozliczalności").

2.8. Administrator wyznacza osobę, której zadaniem jest wspieranie go w realizacji zadań wymienionych w niniejszej Polityce i jej załącznikach, powierzając jej funkcję KODO i zapewnia jej adekwatne środki oraz zasoby niezbędne do wykonywania zleconych jej zadań. W przypadku braku wyznaczenia KODO przez Administratora, obowiązki przypisane w Polityce KODO należy uznać za ciążące na Administratorze.

2.9. Wdrożenie Polityki ma na celu zapewnienie zgodności z RODO procesów przetwarzania przez Administratora Danych osobowych, bez względu na formę (elektroniczną bądź papierową), w jakiej to przetwarzanie następuje.

3. OBOWIĄZKI OSÓB ZAANGAŻOWANYCH W PROCES PRZETWARZANIA DANYCH OSOBOWYCH (STRUKTURA ORGANIZACYJNA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH)

3.1. Za przetwarzanie Danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, innych przepisów dotyczących ochrony Danych osobowych, Polityki a także obowiązujących u Administratora innych wewnętrznych procedur z zakresu ochrony Danych osobowych odpowiadają: Administrator, KODO, Zespół IT, Osoby upoważnione do przetwarzania danych.

3.2. Administrator jest odpowiedzialny za:

3.2.1. zapewnienie odpowiednich środków organizacyjnych i technicznych aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności Podmiotów danych oraz w celu zapewnienia i wykazania przetwarzania Danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania Danych osobowych,

3.2.2. wdrożenie odpowiednich procedur ochrony Danych osobowych,

3.2.3. jeśli uzna to za konieczne, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako element dla stwierdzenia przestrzegania przez Administratora ciążących na nim obowiązków,

3.2.4. zapewnienie środków umożliwiających prawidłową realizację praw Podmiotów danych,

3.2.5. prowadzenie rejestru czynności przetwarzania Danych osobowych,

3.2.6. prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,

3.2.7. współpracę z Organem Nadzorczym w ramach wykonywania przez niego swoich zadań,

3.2.8. zgłaszanie Naruszeń ochrony danych osobowych właściwemu Organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również Podmiotowi danych,

3.2.9. dokumentowanie wszelkich Naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,

3.2.10. zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony Danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultację z Organem nadzorczym,

3.2.11. nadawanie upoważnień do przetwarzania Danych osobowych oraz prowadzenie ewidencji Osób upoważnionych do przetwarzania danych osobowych,

3.2.12. zapewnienie legalności przekazywania Danych osobowych do podmiotów trzecich,

3.2.13. monitorowanie wewnętrznego przestrzegania RODO, innych przepisów prawnych dotyczących ochrony Danych osobowych i wewnętrznych procedur, m.in. poprzez wykonywanie lub zlecanie okresowych audytów.

3.2.14. zapewnienie, że KODO jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony Danych osobowych,

3.2.15. wspieranie KODO w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do Danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,

3.2.16. zagwarantowanie, by KODO nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań.

3.3. Każda Osoba upoważniona do przetwarzania danych zobowiązana jest do:

3.3.1. ochrony Danych osobowych w sposób zgodny z przepisami RODO, innymi przepisami o ochronie Danych osobowych, Polityką i innymi wewnętrznymi procedurami z zakresu ochrony Danych osobowych obowiązujących u Administratora;

3.3.2. zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia; obowiązek ten istnieje także po ustaniu zatrudnienia bez względu na podstawę;

3.3.3. udziału w wewnętrznych i zewnętrznych szkoleniach z zakresu ochrony Danych organizowanych przez Administratora;

3.3.4. podporządkowania się poleceniom Administratora.

3.4. Naruszenie obowiązku ochrony Danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy może potencjalnie skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy bądź rozwiązania stosunku cywilnoprawnego.

3.5. Obowiązki KODO:

3.5.1. monitorowanie zgodności dokumentacji dotyczącej ochrony Danych osobowych i polityk z obowiązującymi przepisami, wytycznymi i orzeczeniami,

3.5.2. udział w projektach biznesowych zgodnie z podejściem privacy by design,

3.5.3. uczestnictwo w procesie szacowania ryzyka w ramach dokonywania oceny skutków dla ochrony danych,

3.5.4. konsultacje dotyczące realizacji wymogów RODO i innych przepisów dotyczących ochrony Danych osobowych dla przedstawicieli działów,

3.5.5. pomoc w kontaktach z Organem nadzorczym, w tym w przypadku potrzeby konsultacji lub zgłoszenia incydentu,

3.5.6. pomoc w kontaktach z Podmiotami danych oraz wsparcie przy przygotowywaniu odpowiedzi na wpływające pytania i żądania,

3.5.7. budowanie świadomości i szkolenie Osób upoważnionych do przetwarzania danych osobowych.

3.6. Obowiązki Zespołu IT:

3.6.1. nadawanie i odwoływanie użytkownikom (w tym użytkownikom uprawnionym do przetwarzania danych) uprawnień w Systemach informatycznych i dostępu do pomieszczeń na polecenie Administratora, pracownika działu HR lub innej osoby upoważnionej przez Administratora do podejmowania decyzji w tym obszarze,

3.6.2. zapewnienie funkcjonowania mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do Danych osobowych.

3.6.3. nadzór nad prawidłowym działaniem Systemów informatycznych (w tym także nad systemami dostarczanymi przez zewnętrznych dostawców),

3.6.4. zapewnienie monitorowania bezpieczeństwa przetwarzania danych w Systemach informatycznych (w tym elementów infrastruktury informatycznej).

3.6.5. kontrola, czy hasła są regularnie zmieniane przez użytkowników, którym zostały nadane uprawnienia w Systemach informatycznych,

3.6.6. regularna kontrola stanu zabezpieczeń Systemu informatycznego przed dostępem do nich osób nieuprawnionych,

3.6.7. podejmowanie działań mających na celu zapewnienie bezpieczeństwa Systemu informatycznego, w którym przetwarzane są Dane osobowe oraz przeciwdziałanie i zapobieżenie dostępowi osób nieuprawnionych do tego systemu.

3.6.8. stosowanie środków ochrony Systemu informatycznego przed szkodliwym oprogramowaniem.

3.6.9. instalację wygaszaczy ekranów na stanowiskach, na których przetwarzane są Dane osobowe.

3.6.10. zgłaszanie KODO oraz Administratorowi wszelkich sytuacji stwierdzenia lub podejrzenia fizycznej ingerencji w przetwarzane Dane osobowe bądź użytkowane narzędzia programowe lub sprzętowe a także podejmowanie odpowiednich działań w przypadku Naruszenia ochrony danych osobowych lub innego incydentu naruszenia bezpieczeństwa,

3.6.11. wykonywanie kopii zapasowych oraz ich okresowe sprawdzanie pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu,

3.6.12. nadzór nad realizacją napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisywane są Dane osobowe,

3.6.13. podejmowanie odpowiednich działań w przypadku Naruszenia ochrony danych osobowych lub innego incydentu naruszenia bezpieczeństwa,

3.6.14. wykonywanie żądań Podmiotów danych w bazie danych Systemu informatycznego, zgodnie z instrukcjami KODO lub Administratora.

4. DOPUSZCZENIE OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH. PROCEDURA NADAWANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

4.1. Przed udzieleniem dostępu do przetwarzania Danych osobowych Administrator zapoznaje każdego Pracownika lub inne osoby przetwarzające dane z jego upoważnienia lub w jego imieniu, z procedurami i zasadami dotyczącymi ochrony Danych osobowych obowiązującymi u Administratora.

4.2. Przetwarzanie Danych osobowych przez Pracowników może odbywać się wyłącznie na podstawie udokumentowanego upoważnienia Administratora, którego zakres odpowiada przypisanej roli i zakresowi odpowiedzialności. Ponadto Administrator zobowiązuje Osoby upoważnione do przetwarzania danych osobowych do zachowania poufności Danych osobowych oraz informacji dotyczących zabezpieczeń danych, a także do przestrzegania procedur i polityk dotyczących ochrony Danych osobowych obowiązujących w organizacji Administratora. Administrator upoważni KODO oraz wybrane osoby z działu HR do udzielania w jego imieniu upoważnień do przetwarzania danych osobowych

4.3. Osobą odpowiedzialną za administrowanie oraz kontrolę upoważnień do przetwarzania danych osobowych są KODO oraz wybrane osoby z działu HR.

4.4. W przypadku zatrudnienia nowego Pracownika, który w ramach swoich obowiązków lub odpowiednio usług/zlecenia będzie przetwarzał Dane osobowe, istnieje konieczność nadania mu stosownego upoważnienia do przetwarzania Danych osobowych. To samo dotyczy sytuacji, w której dochodzi do zmiany stanowiska Pracownika, która łączy się z uzyskaniem dostępu do Danych osobowych.

4.5. Upoważnienie jest wydawane w formie elektronicznej lub papierowej. Wzory upoważnień stanowią Załącznik 1a (dla Pracowników), Załącznik 1b (dla Pracowników przetwarzających Szczególne kategorie Danych osobowych) i Załącznik 1c (dla zleceniobiorców, usługodawców i współpracowników).

4.6. Upoważnienie w postaci elektronicznej nie wymaga odręcznego podpisu osoby upoważniającej oraz upoważnianego. Otrzymanie upoważnienia nadanego w postaci elektronicznej powinno zostać potwierdzone przez Pracownika również w formie elektronicznej i uzupełnione o: (i) informację, że Pracownik zapoznał się z treścią upoważnienia; oraz (ii) treść oświadczenia zawartego we wzorze upoważnienia lub stwierdzenie, że Pracownik składa oświadczenie o treści znajdującej się w nadanym mu upoważnieniu. Upoważnienia w postaci elektronicznej wraz z odpowiedzią Pracownika przechowywane są w formacie .pdf na serwerach Administratora z możliwością wydruku na każde żądanie.

4.7. W przypadku upoważnień w wersji papierowej, wymagają one odręcznego podpisu osoby upoważniającej oraz upoważnianego. Oryginał upoważnienia do przetwarzania Danych osobowych w formie papierowej przechowywany jest przez dział HR.

4.8. Wydanie każdego upoważnienia odnotowywane jest przez dział HR w ewidencji osób upoważnionych do przetwarzania danych osobowych. Ewidencja prowadzona jest w formie elektronicznej zgodnie ze wzorem stanowiącym Załącznik nr 2 do Polityki.

4.9. Zakres nadanego upoważnienia może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez upoważnionego określonych zadań w określonym przedziale czasu.

4.10. W przypadku zmiany stanowiska pracy lub odpowiednio zakresu usług lub zlecenia łączącej się ze zmianą zakresu Danych osobowych, które przetwarza Pracownik istnieje konieczność złożenia wniosku o zmianę upoważnienia. Zmiana zakresu wydanego upoważnienia jest odnotowywana w ewidencji upoważnień.

4.11. Utrata prawa do przetwarzania Danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:

4.11.1. zmiany stanowiska na stanowisko, na którym nie ma konieczności posiadania dostępu do Danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania Danych osobowych w związku ze zmianą realizowanych przez Pracownika zadań wynikających z jego indywidualnego zakresu czynności,

4.11.2. umyślnego i rażącego naruszenia zasad ochrony Danych osobowych określonych w Ustawie, RODO, innych przepisach dotyczących ochrony Danych osobowych lub Polityce,

4.11.3. rozwiązania stosunku pracy,

4.11.4. rozwiązania umowy cywilnoprawnej.

4.12. Odwołanie upoważnienia następuje poprzez jego wycofanie z ewidencji upoważnień oraz powiadomienie w formie elektronicznej lub papierowej upoważnionego. Obowiązek zawiadomienia o cofnięciu upoważnienia nie dotyczy sytuacji, gdy jest ono skutkiem rozwiązania stosunku pracy lub umowy cywilnoprawnej.

5. ZAKRES I CEL PRZETWARZANIA

5.1. Spółka może przetwarzać Dane osobowe osób takich jak pracownicy, dawni pracownicy i członkowie ich rodzin, pracownicy tymczasowi, osoby samozatrudnione, kandydaci do pracy, wykonawcy, osoby kontaktowe z firm dostawczych, kontrahenci, klienci i goście.

5.2. Spółka przetwarza Dane osobowe w celach obejmujących m.in.:

5.2.1. administrację płac i świadczeń;

5.2.2. realizację procesów kadrowych;

5.2.3. ocenę wydajności pracowników i zarządzanie talentami;

5.2.4. marketing i PR;

5.2.5. poprawę produktów i usług biznesowych;

5.2.6. badania i analizy statystyczne;

5.2.7. strategię biznesową;

5.2.8. audyty lub dochodzenia wewnętrzne;

5.2.9. zapobieganie i wykrywanie zachowań niezgodnych z prawem lub procedurami i regulacjami wewnętrznymi Spółki ;

5.2.10. wypełnianie zobowiązań prawnych.

5.2.11. realizację procesu zakupowego;

5.2.12. realizację działań administracyjnych;

5.2.13. realizację obowiązków wynikających z przepisów prawa w szczególności z zakresu prawa podatkowego, o rachunkowości oraz bezpieczeństwa i higieny pracy;

5.2.14. dochodzenie roszczeń lub obronę przed roszczeniami.

5.3. Spółka informuje osoby, których Dane osobowe przetwarza, o celu i zakresie przetwarzania oraz o przysługującym tym osobom prawach, a w razie konieczności wynikającej z przepisów prawa, uzyskuje ich uprzednią i dobrowolną zgodę na przetwarzanie Danych osobowych.

6. RODZAJE PRZETWARZANYCH DANYCH OSOBOWYCH

[Pracownicy i wykonawcy]

6.1. Administrator przetwarza Dane osobowe następujących kategorii Podmiotów danych:

6.1.1. swoich pracowników;

6.1.2. członków ich rodzin (jeżeli podanie ich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy);

6.1.3. kandydatów do pracy;

6.1.4. byłych pracowników;

6.1.5. a także osób świadczących aktualnie lub w przeszłości usługi na rzecz Spółki na podstawie umowy cywilnoprawnej.

6.2. Takie Dane osobowe mogą obejmować: imię i nazwisko, datę urodzenia, numer PESEL, numer NIP, numer konta bankowego, dane dotyczące paszportu i wiz; dane kontaktowe (np. adres korespondencyjny/zamieszkania, numer telefonu); warunki zatrudnienia, informacje dotyczące szkoleń, oceny pracownika, awansów, planów rozwoju osobistego, informacje dotyczące wynagrodzenia; historię wykształcenia i zatrudnienia; informacje medyczne (np. zaświadczenia lekarskie i zwolnienia lekarskie) – gdy jest to wymagane prawem; dane dotyczące emerytury itd.

6.3. Powyższa lista nie odnosi się w równym stopniu do każdej kategorii Podmiotów danych i nie jest kompletną listą wszystkich Danych osobowych, lecz obejmuje te, które są najczęściej przetwarzane przez Spółkę.

[Dostawcy, klienci, kontrahenci]

6.4. Administrator przetwarza Dane osobowe następujących kategorii Podmiotów danych:

6.4.1. osób będących jego dostawcami, klientami, kontrahentami.

6.4.2. osób pracujących lub współpracujących z jego dostawcami, klientami, kontrahentami.

6.4.3. reprezentantów jego dostawców, klientów, kontrahentów.

6.5. Podczas przetwarzania Danych osobowych wyżej wymienionych kategorii osób, Spółka może wystąpić w roli Administratora tych danych, a w niektórych przypadkach jako Podmiot przetwarzający te dane w imieniu innego administratora, który udostępnił te dane Spółce na podstawie umowy powierzenia przetwarzania.

6.6. Takie Dane osobowe mogą obejmować: służbowe dane identyfikacyjne, takie jak, np. imię, nazwisko, nazwa stanowiska służbowego, robocze numery identyfikacyjne, dział, firmę, służbowe dane kontaktowe, takie jak, np. numer telefonu służbowego, służbowy adres e-mail, a także numer PESEL, numer prawa jazdy, dokumenty potwierdzające posiadanie wymaganych prawem uprawnień zawodowych lub odbytych szkoleń, numer NIP, numer VAT.

6.7. Powyższa lista nie odnosi się w równym stopniu do każdej kategorii Podmiotów danych i nie jest kompletną listą wszystkich Danych osobowych, lecz obejmuje te, które są najczęściej przetwarzane przez Spółkę.

6.8. Jeżeli przetwarzanie przez Spółkę Danych osobowych wyżej wymienionych kategorii osób odbywa się na podstawie powierzenia jej przetwarzania tych danych, Spółka może przetwarzać je wyłącznie według sposobu, zakresu i celu określonego przez administratora. Jedynym odstępstwem od powyższej zasady jest sytuacja, w której przepis powszechnie obowiązującego prawa będzie zobowiązywał Spółkę do przetwarzania powierzonych jej Danych osobowych w sposób inny niż określony przez administratora, np. w zakresie okresu przechowywania tych danych lub ich udostępnienia podmiotom uprawnionym do ich otrzymania.

[Szczególne kategorie Danych osobowych]

6.9. W przypadku, gdy Spółka przetwarza Szczególne kategorie Danych osobowych przetwarzanie to odbywa się zgodnie z przepisami dotyczącymi ochrony Danych osobowych, w szczególności z art. 9 ust. 2 RODO.

7. ORGANIZACJA SYSTEMU OCHRONY DANYCH OSOBOWYCH

7.1. Podmiotem ponoszącym ogólną odpowiedzialność za zgodność Spółki z Polityką jest zarząd Spółki. Spółka wspierana jest przez KODO, dział IT oraz dział prawny (jeśli zostały one powołane lub utworzone w Spółce).

7.2. Administrator przypisuje role i zakres odpowiedzialności w procesie przetwarzania Danych osobowych każdemu z uczestników tego procesu.

7.3. Administrator:

7.3.1. informuje Pracowników, którzy przetwarzają Dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i innych przepisów unijnych lub krajowych o ochronie Danych osobowych, jak również zapewnia doradztwo w kwestiach powiązanych;

7.3.2. monitoruje przestrzeganie przez Osoby upoważnione do przetwarzania danych osobowych przepisów RODO oraz innych przepisów unijnych i krajowych z zakresu ochrony Danych osobowych, jak również wewnętrznych polityk i procedur wdrożonych u Administratora w tym zakresie;

7.3.3. przestrzega realizacji innych obowiązków wynikających z RODO oraz innych przepisów unijnych i krajowych z zakresu ochrony Danych osobowych.

7.4. Administrator przetwarza Dane osobowe z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

7.5. Pracownicy przetwarzający Dane osobowe są zobowiązani w szczególności do:

7.5.1. przetwarzania Danych osobowych zgodnie z posiadanym upoważnieniem oraz z należytą starannością;

7.5.2. w przypadku zaobserwowania zdarzenia mogącego stanowić Naruszenie ochrony danych osobowych, niezwłocznego informowania o nim bezpośredniego przełożonego oraz KODO (jeśli został wyznaczony) na zasadach opisanych w Procedurze oceny i notyfikacji naruszeń ochrony danych osobowych;

7.5.3. uczestnictwa w organizowanych szkoleniach z zakresu ochrony Danych osobowych;

7.5.4. zachowania w poufności Danych osobowych oraz informacji na temat sposobu ich zabezpieczenia, zgodnie z podpisaną klauzulą poufności lub innymi dokumentami.

8. UDOSTĘPNIANIE I POWIERZANIE DANYCH OSOBOWYCH

8.1. Administrator w uzasadnionych i dozwolonych prawnie przypadkach może udostępniać lub przekazywać Dane osobowe do przetwarzania podmiotom trzecim. Spółka w ramach prowadzonej działalności przekazuje Dane osobowe następującym kategoriom podmiotów:

8.1.1. podmiotom z grupy spółek, do której należy także Administrator;

8.1.2. usługodawcom, partnerom biznesowym, dostawcom i podwykonawcom;

8.1.3. podmiotom upoważnionym do uzyskania wglądu w Dane osobowe na podstawie przepisów prawa, jeżeli Spółka podlega prawnemu obowiązkowi udostępnienia takich Danych osobowych.

8.2. Udostępnianie Danych osobowych jest dopuszczalne tylko wtedy, gdy spełniony jest jeden z warunków, o którym mowa w art. 6 ust. 1 albo w art. 9 ust. 2 RODO.

8.3. Powierzenie przetwarzania Danych osobowych podmiotowi trzeciemu następuje w oparciu o umowę powierzenia przetwarzania danych osobowych, po weryfikacji tego podmiotu w sposób określony w Polityce wyboru dostawcy przetwarzającego dane osobowe. Zawierana przez Administratora umowa powierzenia przetwarzania Danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:

8.3.1. przedmiot powierzenia,

8.3.2. czas trwania powierzenia,

8.3.3. charakter i cel przetwarzania,

8.3.4. rodzaj powierzanych Danych osobowych,

8.3.5. kategorie Podmiotów danych,

8.3.6. warunki podpowierzenia przetwarzania Danych osobowych,

8.3.7. obowiązki i prawa Administratora,

8.3.8. obowiązki Podmiotu przetwarzającego.

8.4. W przypadku, gdy elementy powierzenia przetwarzania Danych osobowych wskazane w pkt 8.3. znajdują się już w zawartej z danym podmiotem umowie, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania Danych osobowych.

8.5. Za zawieranie umów powierzenia przetwarzania Danych osobowych odpowiadają pracownicy upoważnieni do przetwarzania Danych osobowych u Administratora.

8.6. Każdy Pracownik przed planowanym rozpoczęciem współpracy z Podmiotem przetwarzającym, jest zobowiązany poinformować o tym KODO (jeśli został wyznaczony przez Spółkę) oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania Danych osobowych.

8.7. Każdorazowe dokonanie powierzenia przetwarzania Danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania Danych osobowych.

8.8. Administrator ma prawo kontroli Podmiotów przetwarzających, którym powierzył przetwarzanie Danych osobowych.

8.9. Administrator w zakresie prowadzonej przez siebie działalności może przetwarzać również Dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie Danych osobowych w powierzenie przez Spółkę musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania Danych osobowych.

9. WSPÓŁADMINISTROWANIE DANYMI

9.1. Administrator w zakresie przetwarzanych przez siebie Danych osobowych dopuszcza możliwość współadministrowania Danymi osobowymi zgodnie z art. 26 RODO.

9.2. Współadministrowanie Danymi osobowymi może zachodzi wówczas, jeżeli Administrator oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania Danych osobowych.

9.3. Aby doszło do współadministrowania w danym procesie przetwarzania Danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator oraz co najmniej jeden inny podmiot muszą:

9.3.1. być administratorami w rozumieniu art. 4 pkt 7 RODO,

9.3.2. muszą wspólnie ustalać cele przetwarzania Danych osobowych,

9.3.3. muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania Danych osobowych.

9.4. W przypadku spełnienia warunków, o których mowa w pkt 9.3 Administrator oraz co najmniej jeden inny podmiot stają się współadministratorami Danych osobowych w zakresie danego procesu przetwarzania.

9.5. W przypadku przyjęcia modelu współadministrowania Danymi osobowymi, współadministratorzy w drodze wspólnych uzgodnień umownych, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

9.6. W sytuacji, kiedy w zakresie zachodzących w strukturze Administratora procesów przetwarzania Danych osobowych pojawią się procesy, wobec których istnieje prawdopodobieństwo zachodzenia współadministrowania danymi, Pracownik zaangażowany w proces informuje o tym fakcie KODO (jeśli został wyznaczony przez Spółkę).

9.7. KODO, a w przypadku braku jego wyznaczenia - każdy Pracownik przed planowanym rozpoczęciem współpracy z podmiotem trzecim (potencjalnym współadministratorem)dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania Danymi osobowymi.

9.8. W przypadku, kiedy wynik oceny, o której mowa w pkt 9.7 wskazuje na współadministrowanie danymi osobowymi, KODO lub właściwy Pracownik, przy współudziale pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w pkt 9.4.

10. PRZEKAZYWANIE DANYCH OSOBOWYCH POZA EOG

10.1. Poziom ochrony Danych osobowych poza EOG (Transgraniczne przetwarzanie) różni się od tego zapewnianego przez prawo europejskie. Z tego powodu Administrator przekazuje Dane osobowe poza EOG tylko wtedy, gdy jest to konieczne i z zapewnieniem odpowiedniego stopnia ochrony, przede wszystkim poprzez:

10.1.1. współpracę z Podmiotami przetwarzającymi Dane osobowe w państwach, w odniesieniu do których została wydana stosowna decyzja Komisji Europejskiej dotycząca stwierdzenia zapewnienia odpowiedniego stopnia ochrony Danych osobowych;

10.1.2. stosowanie standardowych klauzul umownych wydanych przez Komisję Europejską;

10.1.3. stosowanie wiążących reguł korporacyjnych, zatwierdzonych przez właściwy Organ nadzorczy;

10.1.4. przeprowadzenie oceny skutków transferów danych.

10.2. Administrator zawsze informuje o zamiarze przekazania Danych osobowych poza EOG w klauzulach informacyjnych na etapie ich zbierania.

10.3. Każdy Pracownik przed planowanym przekazaniem Danych osobowych poza EOG, jest zobowiązany poinformować o tym KODO (jeśli został wyznaczony przez Spółkę) oraz skonsultować z nim warunki przekazania tych danych.

11. NARUSZENIA OCHRONY DANYCH OSOBOWYCH

11.1. Administrator zapewnia zgłaszanie Naruszeń ochrony danych osobowych Organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W tym celu Administrator w szczególności zobowiązuje wszystkie osoby przetwarzające Dane osobowe do niezwłocznego informowania o każdym dostrzeżonym Naruszeniu ochrony danych osobowych zgodnie z Procedurą oceny i notyfikacji naruszeń ochrony danych osobowych.

11.2. W każdym wypadku Administrator bada zaistniałe naruszenie i wdraża stosowne organizacyjne i techniczne środki naprawcze.

12. PRAWA PODMIOTÓW DANYCH I KONTAKT Z PODMIOTAMI DANYCH

12.1. Administrator wdraża odpowiednie środki, aby komunikacja z Podmiotem danych odbywała się w zwięzłej, przejrzystej i łatwo dostępnej formie.

12.2. Przyjmowanie i obsługa żądań Podmiotów danych odbywa się na zasadach określonych w Procedurze obsługi żądań Podmiotów danych dotyczących realizacji praw związanych z przetwarzaniem Danych osobowych.

12.3. Podmiotom danych przysługują następujące prawa:

12.3.1. **prawo do informacji o przetwarzaniu Danych osobowych** – na tej podstawie Administrator przekazuje osobie fizycznej zgłaszającej żądanie informację o przetwarzaniu Danych osobowych, w tym przede wszystkim o celach i podstawach prawnych przetwarzania, zakresie posiadanych danych, podmiotach, którym są ujawniane, i planowanym terminie usunięcia danych;

12.3.2. **prawo uzyskania kopii Danych osobowych** – na tej podstawie Administrator przekazuje kopię przetwarzanych danych dotyczących osoby fizycznej zgłaszającej żądanie;

12.3.3. **prawo do sprostowania** – Administrator zobowiązany jest usuwać ewentualne niezgodności lub błędy przetwarzanych Danych osobowych oraz uzupełniać je, jeśli są niekompletne;

12.3.4. **prawo do usunięcia Danych osobowych** – na tej podstawie można żądać usunięcia Danych osobowych, których przetwarzanie nie jest już niezbędne do realizowania żadnego z celów, dla których zostały zebrane;

12.3.5. **prawo do ograniczenia przetwarzania** – w razie zgłoszenia takiego żądania Administrator zaprzestaje wykonywania operacji na Danych osobowych w zakresie objętym żądaniem – z wyjątkiem operacji, na które wyraziła zgodę osoba, której dane dotyczą, – lub dopóki nie ustaną przyczyny ograniczenia przetwarzania danych (np. zostanie wydana decyzja Organu nadzorczego zezwalająca na dalsze przetwarzanie danych);

12.3.6. **prawo do przenoszenia Danych osobowych** – na tej podstawie – w zakresie, w jakim Dane osobowe są przetwarzane w sposób zautomatyzowany w związku z zawartą umową lub wyrażoną zgodą – Administrator wydaje dane dostarczone przez osobę, której one dotyczą, w formacie pozwalającym na odczyt Danych osobowych przez komputer. Możliwe jest także zażądanie przesłania tych danych innemu podmiotowi, jednakże pod warunkiem, że istnieją w tym zakresie techniczne możliwości zarówno po stronie Administratora, jak również wskazanego podmiotu;

12.3.7. **prawo sprzeciwu wobec przetwarzania Danych osobowych w celach marketingowych** – Podmiot danych może w każdym momencie sprzeciwić się przetwarzaniu Danych osobowych w celach marketingowych, bez konieczności uzasadnienia takiego sprzeciwu;

12.3.8. **prawo sprzeciwu wobec innych celów przetwarzania Danych osobowych** – Podmiot danych może w każdym momencie sprzeciwić się – z przyczyn związanych z jego szczególną sytuacją – przetwarzaniu Danych osobowych, które odbywa się na podstawie prawnie uzasadnionego interesu Administratora (np. dla celów analitycznych lub statystycznych albo ze względów związanych z ochroną mienia);

12.3.9. **prawo wycofania zgody** – jeśli Dane osobowe przetwarzane są na podstawie wyrażonej zgody, Podmiot danych ma prawo wycofać ją w dowolnym momencie, co jednak nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem;

12.3.10. **prawo do skargi** – w przypadku uznania, że przetwarzanie Danych osobowych narusza przepisy RODO lub inne przepisy dotyczące ochrony Danych osobowych, Podmiot danych może złożyć skargę do Organu nadzorczego, właściwego ze względu na miejsce zwykłego pobytu Podmiotu danych, jego miejsce pracy lub miejsce popełnienia domniemanego naruszenia. W Polsce właściwym Organem nadzorczym jest PUODO.

12.4. Realizacja praw Podmiotów danych nie ma charakteru bezwzględnego. Przed spełnieniem żądania osoba rozpatrująca wniosek Podmiotu danych powinna zweryfikować, czy zachodzą przesłanki wyłączające spełnienia żądania (np. istnienie innej ważnej podstawy prawnej dalszego przetwarzania Danych osobowych objętych żądaniem).

13. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

13.1. Dane osobowe są przechowywane z zachowaniem odpowiedniego poziomu zabezpieczeń za pomocą różnych środków bezpieczeństwa.

13.2. Spółka stosuje środki techniczne, organizacyjne, fizyczne i logiczne w celu ochrony Danych osobowych przed bezprawnym lub nieupoważnionym zniszczeniem, utratą, zmianą, ujawnieniem, nabyciem i dostępem do nich, w szczególności:

13.2.1. zabezpieczenia organizacyjne, tj. środki organizacyjne oraz wymagania dotyczące polityki zarządzania procesem przetwarzania, w tym zastosowanych procedur,

13.2.2. zarządzanie projektem,

13.2.3. zarządzanie incydentami,

13.2.4. zarządzanie personelem,

13.2.5. zarządzanie udziałem stron trzecich, w tym Podmiotów przetwarzających,

13.2.6. zarządzanie eksploatacją używanych Systemów informatycznych i innych narzędzi przetwarzania Danych osobowych,

13.2.7. nadzór, w tym audyty i raportowanie alertów.

13.3. środki kontroli logicznej procesu przetwarzania, w tym wymagania dotyczące zastosowania takich środków ochrony, jak:

13.3.1. anonimizacja i pseudonimizacja,

13.3.2. środki ochrony kryptograficznej,

13.3.3. środki kontroli integralności danych,

13.3.4. środki kontroli dostępu do danych,

13.3.5. środki kontroli dotyczące rozliczalności wykonywanych operacji,

13.3.6. środki wspierające weryfikację danych na etapie ich wprowadzania, typu: zgodność z wzorcem, podanymi wartościami granicznymi itp.,

13.3.7. środki bieżącego monitoringu,

13.3.8. zastosowane środki ochrony przed działaniem oprogramowania szkodliwego typu wirusy, środki szpiegujące, środki służące ochronie przed wykradaniem danych, itp.

13.3.9. środki ochrony sieci przed działaniem osób z zewnątrz.

13.4. środki ochrony fizycznej wszystkich aktywów informacyjnych i technicznych, w tym:

13.4.1. środków bezpieczeństwa infrastruktury technicznej wykorzystywanej do przetwarzania danych,

13.4.2. środków bezpieczeństwa dokumentacji papierowej, w tym papierowych rejestrów zawierających dane osobowe,

13.4.3. środków bezpieczeństwa związanych z przepływem informacji w postaci dokumentów papierowych lub nośników elektronicznych,

13.4.4. środków ochrony przed żywiołami niezależnymi od człowieka, typu ogień, woda.

13.5. Kwestie związane z przetwarzaniem danych osobowych w systemach informatycznych i ich ochroną opisuje Polityka Bezpieczeństwa Informacji , stanowiąca załącznik do Polityki.

14. GLOBALNA POLITYKA BEZPIECZEŃSTWA INFORMACJI CRH

14.1. Podstawowymi celami Globalnej Polityki Bezpieczeństwa Informacji CRH są:

14.1.1. identyfikacja ryzyk bezpieczeństwa informacji związanych z nieuprawnionym dostępem, niewłaściwym użyciem, modyfikacją lub zniszczeniem aktywów informacyjnych, zarządzanie nimi oraz wdrożenie środków kontroli, mających na celu ograniczenie wpływu tych ryzyk,

14.1.2. zapewnienie zgodności z lokalnymi przepisami ustawowymi i regulacjami. Uwaga: jeżeli lokalne przepisy i regulacje są bardziej rygorystyczne niż środki kontroli przewidziane w niniejszej Polityce, wówczas takie lokalne przepisy i regulacje będą mieć pierwszeństwo w stosunku do niniejszej Polityki,

14.1.3. wzmocnienie i poprawa poziomu świadomości oraz dojrzałości w zakresie bezpieczeństwa informacji w skali całej Spółki.

14.2. Globalna Polityka Bezpieczeństwa Informacji CRH jest polityką szerszą, obejmującą swym zakresem wszelkie dane przetwarzane w Spółce, w tym także Dane osobowe. W związku z tym, Globalna Polityka Bezpieczeństwa Informacji CRH jest dokumentem nadrzędnym w

stosunku do Polityki ochrony danych, chyba że Polityka ochrony danych przewiduje bardziej restrykcyjną ochronę danych osobowych.

15. ZAPEWNIENIE CIĄGŁOŚCI

15.1. Administrator zapewnia stałe monitorowanie zgodności działania Spółki z zasadami ochrony Danych osobowych.

15.2. Do podejmowania czynności związanych z zapewnieniem zgodności zobowiązany jest KODO (jeśli został wyznaczony przez Spółkę). Każdy Pracownik Spółki zobowiązany jest wspierać KODO w wykonywaniu jego zadań, w szczególności udzielać niezbędnych informacji i wyjaśnień.

16. POSTANOWIENIA KOŃCOWE

16.1. Polityka jest aktualizowana przez Administratora w zależności od potrzeb. KODO oraz Pracownicy (jeśli KODO nie został wyznaczony) są uprawnieni do składania wniosku o aktualizację Polityki. Zasady aktualizacji poszczególnych załączników Polityki określone są w tych załącznikach.

16.2. Polityka wchodzi w życie z dniem wskazanym w uchwale Zarządu.

16.3. Załączniki:

- **16.3.1.** Załącznik 1a - wzór upoważnienia do przetwarzania danych dla pracownika
- **16.3.2.** Załącznik 1b - wzór upoważnienia do przetwarzania danych dla pracownika przetwarzającego Szczególne kategorie Danych osobowych
- **16.3.3.** Załącznik 1c - wzór upoważnienia do przetwarzania danych dla zleceniobiorców, usługodawców i współpracowników
- **16.3.4.** Załącznik 2 – Wzór ewidencji osób upoważnionych
- **16.3.5.** Załącznik 3 - Globalna Polityka Bezpieczeństwa Informacji CRH.

Warszawa, ……..

(administrator danych osobowych)

(miejscowość, data)

UPOWAŻNIENIE NR [●]/2024

My, niżej podpisani, upoważniamy:

[●]
Imię i nazwisko upoważnianego

[●]
Stanowisko służbowe upoważnianego

do przetwarzania danych osobowych w ramach powierzonych obowiązków wynikających **z umowy o pracę/stanowiskowej karty obowiązków pracowniczych** oraz do wykonania zadań zleconych przez przełożonego.

Zakres upoważnienia obejmuje przetwarzanie:
(i) wyłącznie danych osobowych, które nie stanowią szczególnych kategorii danych osobowych[1];
(ii) danych w wersji papierowej oraz elektronicznej, w zakresie zbierania, utrwalania, organizowania, porządkowania, przechowywania, adaptowania lub modyfikowania, pobierania, przeglądania, wykorzystywania, ujawniania poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie *(niepotrzebne skreślić)*;
(iii) danych osobowych następujących kategorii osób fizycznych: *(należy wskazać, np. pracownicy, współpracownicy, dostawcy, kontrahenci)*.

Zakres upoważnienia do przetwarzania danych w systemach informatycznych jest określony poprzez indywidualnie przyznawane uprawnienia dostępu do każdego systemu.

W przypadku uzyskania przez Pana/Panią dostępu do szczególnych kategorii danych osobowych należy zgłosić tę okoliczność do koordynatora ds. ochrony danych osobowych lub, jeśli nie został wyznaczony przez administratora danych osobowych, do bezpośredniego przełożonego.

Jest Pan/Pani zobowiązany(a) do zachowania w tajemnicy przetwarzanych danych osobowych, do których ma lub będzie miał/a Pani/Pan dostęp w związku z wykonywaniem obowiązków służbowych, jak również sposobów ich zabezpieczenia a także do przestrzegania obowiązujących w ……... procedur i polityk dotyczących ochrony danych.

Obowiązek zachowania poufności przetwarzanych danych osobowych oraz informacji dotyczących zabezpieczeń tych danych, istnieje również po wygaśnięciu lub rozwiązaniu umowy z ……

Niniejsze upoważnienie jest ważne do chwili jego odwołania lub zmiany albo ustania umowy.

……
w imieniu administratora

OŚWIADCZENIE

Ja, niżej podpisany/-a, oświadczam, iż zobowiązuję się do zachowania w tajemnicy treści przetwarzanych danych osobowych oraz wszelkich informacji dotyczących sposobów ich zabezpieczenia, zarówno w trakcie wykonywania umowy, jak i po jej ustaniu.
Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania tych przepisów, w tym w szczególności RODO[2], wydanych na ich podstawie aktów wykonawczych, a także obowiązujących w …… z siedzibą w Warszawie dokumentów wewnętrznych.

……
czytelny podpis osoby składającej oświadczenie

[1] *Szczególne kategorie danych osobowych obejmują: (i) dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; (ii) dane dotyczące zdrowia, seksualności lub orientacji seksualnej; (iii) dane genetyczne i biometryczne, o ile wykorzystywane są w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących tej osoby.*

[2] 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.).

Warszawa, ……..

(administrator danych osobowych)

(miejscowość, data)

UPOWAŻNIENIE NR [●]/2024

My, niżej podpisani, upoważniamy:

[●]
Imię i nazwisko upoważnianego

[●]
Stanowisko służbowe upoważnianego

do przetwarzania danych osobowych w ramach powierzonych obowiązków wynikających **z umowy o pracę z dnia……..**

Zakres niniejszego upoważnienia obejmuje przetwarzanie:

(i) zarówno standardowych kategorii danych osobowych, jak i szczególnych kategorii danych osobowych[3];
(ii) danych w wersji papierowej oraz elektronicznej, w zakresie zbierania, utrwalania, organizowania, porządkowania, przechowywania, adaptowania lub modyfikowania, pobierania, przeglądania, wykorzystywania, ujawniania poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie *(niepotrzebne skreślić)*;
(iii) danych osobowych następujących kategorii osób fizycznych: *(należy wskazać, np. pracownicy, współpracownicy, kontrahenci)*.

Zakres upoważnienia do przetwarzania danych w systemach informatycznych jest określony poprzez nadane Panu/Pani uprawnienia w systemach informatycznych wykorzystywanych przy przetwarzaniu tych danych.

Jednocześnie zobowiązujemy wyżej wskazaną osobę do zachowania poufności przetwarzanych danych osobowych oraz informacji dotyczących zabezpieczeń tych danych, a także do przestrzegania obowiązujących w ……. procedur i polityk dotyczących ochrony danych.

Obowiązek zachowania poufności przetwarzanych danych osobowych oraz informacji dotyczących zabezpieczeń tych danych istnieje również po wygaśnięciu umowy lub zakończeniu współpracy z …….

Niniejsze upoważnienie jest ważne do chwili jego odwołania lub zmiany albo ustania umowy.

……
w imieniu administratora

OŚWIADCZENIE

Ja, niżej podpisany/-a, oświadczam, iż zobowiązuję się do zachowania w tajemnicy treści przetwarzanych danych osobowych oraz wszelkich informacji dotyczących sposobów ich zabezpieczenia, zarówno w trakcie wykonywania umowy, jak i po jej ustaniu.
Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania tych przepisów, w tym w szczególności RODO[2], wydanych na ich podstawie aktów wykonawczych, a także obowiązujących w …….. z siedzibą w Warszawie dokumentów wewnętrznych.

……
czytelny podpis osoby składającej oświadczenie

[3] *Szczególne kategorie danych osobowych obejmują: (i) dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; (ii) dane dotyczące zdrowia, seksualności lub orientacji seksualnej; (iii) dane genetyczne i biometryczne, o ile wykorzystywane są w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących tej osoby.*

[2] 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.).

Warszawa, ……..

(administrator danych osobowych)

(miejscowość, data)

UPOWAŻNIENIE NR [●]/2024

My, niżej podpisani, upoważniamy:

[●]
Imię i nazwisko upoważnianego

do przetwarzania danych osobowych w zakresie niezbędnym do realizacji zlecenia lub świadczenia usług wynikających z **umowy o współpracę/umowy zlecenia/ umowy o dzieło z dnia ……** zawartej z …….. z siedzibą w Warszawie.

Zakres upoważnienia obejmuje przetwarzanie:

(iv) wyłącznie danych osobowych, które nie stanowią szczególnych kategorii danych osobowych[4];

(v) danych w wersji papierowej oraz elektronicznej, w zakresie zbierania, utrwalania, organizowania, porządkowania, przechowywania, adaptowania lub modyfikowania, pobierania, przeglądania, wykorzystywania, ujawniania poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie *(niepotrzebne skreślić)*;

(vi) danych osobowych następujących kategorii osób fizycznych: *(należy wskazać, np. pracownicy, współpracownicy, dostawcy, kontrahenci)*.

Zakres upoważnienia do przetwarzania danych w systemach informatycznych jest określony poprzez indywidualnie przyznawane uprawnienia dostępu do każdego systemu.

Jest Pan/Pani zobowiązany(a) do zachowania w tajemnicy przetwarzanych danych osobowych, do których ma lub będzie miał/a Pani/Pan dostęp, jak również sposobów ich zabezpieczenia, a także do przestrzegania obowiązujących w …….. procedur i polityk dotyczących ochrony danych.

Niniejsze upoważnienie jest ważne do chwili jego odwołania lub zmiany albo ustania umowy.

Obowiązek zachowania poufności przetwarzanych danych osobowych oraz informacji dotyczących zabezpieczeń tych danych istnieje również po wygaśnięciu umowy lub zakończeniu współpracy z …….. do czasu utraty przez te informacje wartości gospodarczej, ale nie krócej niż przez okres 3 lat.

……
w imieniu administratora

OŚWIADCZENIE

Ja, niżej podpisany/-a, oświadczam, iż zobowiązuję się do zachowania w tajemnicy treści przetwarzanych danych osobowych oraz wszelkich informacji dotyczących sposobów ich zabezpieczenia, zarówno w trakcie wykonywania umowy, jak i po jej zakończeniu – do czasu utraty przez te informacje wartości gospodarczej, ale nie której niż przez okres 3 lat.
Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania tych przepisów, w tym w szczególności RODO[5], wydanych na ich podstawie aktów wykonawczych, a także obowiązujących w ……. z siedzibą w Warszawie dokumentów wewnętrznych.

……
czytelny podpis osoby składającej oświadczenie

[4] *Szczególne kategorie danych osobowych obejmują: (i) dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; (ii) dane dotyczące zdrowia, seksualności lub orientacji seksualnej; (iii) dane genetyczne i biometryczne, o ile wykorzystywane są w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących tej osoby.*

[5] 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.).

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Dane Administratora	dane spółki grupy CRH w Polsce

l.p.	imię	nazwisko	stanowisko służbowe	identyfikator, jeżeli dane są przetwarzane w systemie informatycznym	dział	data udzielenia upoważnienia	zakres upoważnienia	Data modyfikacji upoważnienia	data ustania upoważnienia (data jego odwołania).	podstawa dla upoważnienia (umowa wiążąca z Administratorem)
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										