Polityka Bezpieczeństwa Danych Osobowych Przedsiębiorstw Holcim w Polsce

§ 1.
PREAMBUŁA

1. Polityka Bezpieczeństwa Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez grupę Przedsiębiorstw Holcim w Polsce, w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (dalej RODO).
2. Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z Rozporządzeniem RODO (§ 1, p.1).
3. Według preambuły rozporządzenia RODO, *„za grupę przedsiębiorstw należy uznać przedsiębiorstwo kontrolujące przetwarzanie danych osobowych w przedsiębiorstwach powiązanych z nim, wraz z tymi przedsiębiorstwami”*.
4. Za spółkę dominującą została uznana spółka **Holcim Polska S.A.** ul. Warszawska 110, 28-366 Małogoszcz, NIP 526-10-60-765, przy czym kryterium uznania za spółkę dominującą jest posiadanie kontroli nad przetwarzaniem danych a nie dominacja kapitałowa czy udziałowa. Aktualny wykaz spółek zależnych oraz powiązanych w ramach Przedsiębiorstw Holcim w Polsce jest udostępniany w siedzibie spółki oraz na stronie www.holcim.pl
5. W zależności od danego stanu faktycznego, każda ze spółek uczestniczących w grupie, może w odniesieniu do niektórych danych być administratorem, a co do niektórych pełnić funkcję procesora.
6. Kryterium decydującym o roli administratora jest decyzyjność w zakresie ustalania celów i sposobów przetwarzania danych osobowych.
7. Spółki w ramach ustalania ładu korporacyjnego przyjmują, że administratorem danych osobowych pracowników będzie ich pracodawca, czyli podmiot, z którym pracownicy nawiązali stosunek pracy.
8. Dane osobowe pracowników będą także przetwarzane przez inne spółki z grupy, na podstawie prawnie usprawiedliwionego celu administratorów.
9. Mapowanie procesów przetwarzania danych zostało przeprowadzone w poszczególnych spółkach grupy kapitałowej i pomiędzy nimi.
10. W wyniku mapowania powstał model przepływu i przetwarzania danych w grupie w postaci rejestru czynności przetwarzania (RCP).
11. Podstawą przesyłania danych w grupie przedsiębiorstw jest punkt 48. preambuły RODO: „*administratorzy, którzy są częścią grupy przedsiębiorstw mogą mieć prawnie uzasadniony interes w przesyłaniu danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników*.
12. W ramach procesu administracji systemami informatycznymi, w tym: kadrowo-płacowymi, finansowymi, sprzedażowymi i zakupowymi, dane osobowe przekazywane są do kraju trzeciego znajdującego się poza Europejskim Obszarem Gospodarczym.
13. Przekazanie danych następuje zgodnie z art. 46 RODO, w szczególności poprzez zawarcie unijnych Standardowych Klauzuli Umownych.

14. Jednym z mechanizmów zabezpieczających przesyłanie danych są wiążące reguły korporacyjne (np. Dyrektywę Holcim o Ochronie Danych).
15. Dokument ten spełnia wymogi określone w RODO oraz jest zatwierdzony przez właściwy organ nadzorczy.

§ 2.
Podstawa prawna

1. Dane osobowe w **Przedsiębiorstwach Holcim w Polsce (Holcim Polska SA oraz spółki zależne)** przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
    a. 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,
    b. przepisów Ustawy z dnia 16 lipca 2004 roku – Prawo Telekomunikacyjne (tj. Dz. U. 2022, poz. 1648 z późn. zm),
    c. przepisów Ustawy z dnia 13 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji (tj. Dz. U. 2022 poz. 1233 z późn. zm.),
    d. przepisów art. 22 § 1-5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tj. Dz.U. 2022, poz. 1510 z późn. zm.) i przepisów wykonawczych wydanych z upoważnienia tej ustawy,
    e. innych przepisów ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii.
2. Dane osobowe w Przedsiębiorstwach Holcim w Polsce przetwarzane są w celu realizacji zadań. W szczególności dane osobowe przetwarza się dla:
    a. zabezpieczenia prawidłowego toku podstawowej działalności, realizacji innych usprawiedliwionych celów i zadań Przedsiębiorstw Holcim w Polsce w zakresie:
        1) planowania, prowadzenia, zarządzania oraz administrowania danymi osobowymi podmiotów danych (lub strony trzeciej, z którą podmioty danych są powiązane) umownymi relacjami biznesowymi, np. poprzez realizację transakcji oraz zamówień produktów lub usług, przetwarzanie płatności, przeprowadzanie czynności rachunkowych, rewizyjnych, rozliczeniowych oraz windykacyjnych, organizowanie wysyłek oraz dostaw, ułatwianie napraw oraz świadczenie usług wspierających oraz zapewnienie innych usług lub rzeczy, o które mogą się podmioty danych do nas zwrócić;
        2) utrzymania bezpieczeństwa oraz ochrony naszych produktów, usług oraz stron internetowych lub innych systemów, zapobiegania oraz wykrywania zagrożeń dla bezpieczeństwa, oszustw oraz innych działań przestępczych lub szkodliwych;
        3) zapewnienia obowiązku przestrzegania zgodności z prawem, takiego jak kontrola przestrzegania przepisów lub obowiązek prowadzenia ewidencji (np. na mocy prawa antymonopolowego, przepisów eksportowych, sankcji handlowych i przepisów dotyczących embarga, przepisów zapobiegających łapówkarstwu i korupcji oraz przepisów wewnętrznych lub by zapobiegać przestępstwom urzędniczym albo praniu brudnych pieniędzy), co może obejmować zautomatyzowane sprawdzenie danych kontaktowych i identyfikacyjnych podmiotów danych na stosownych listach sankcjonowanych stron oraz skontaktowanie się z podmiotami danych w celu potwierdzenia ich tożsamości, w przypadku potencjalnego dopasowania lub zarejestrowanie interakcji podmiotu danych ze stronami trzecimi, co może być istotne dla celów ochrony konkurencji;

4) rozstrzygania sporów, dochodzenia realizacji naszych umów oraz wykazywania zasadności, wniesienia lub obrony roszczeń lub
5) zapewnienia zgodności z wymogami prawnymi np. dotyczącymi prowadzenia dokumentacji sprzedaży do celów podatkowych lub wysyłania powiadomień oraz innych informacji tak jak wymaga tego prawo.

b. zapewnienia prawidłowej, zgodnej z prawem i celami Przedsiębiorstw Holcim w Polsce polityki personalnej oraz bieżącej obsługi stosunków pracy a także innych stosunków zatrudnienia nawiązywanych przez Przedsiębiorstwa Holcim w Polsce.

§ 3.
Podstawowe Definicje

Przez użyte w dokumencie określenia rozumie się:

a. **Przedsiębiorstwa Holcim w Polsce lub Holcim w Polsce** - Holcim Polska S.A. z siedzibą w Małogoszczu, ul. Warszawska 110, 28-366 Małogoszcz (Administrator) oraz spółki zależne. Aktualny wykaz spółek zależnych oraz powiązanych jest udostępniany w siedzibie spółki oraz na stronie www.holcim.pl
b. **Administrator (danych)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
c. **RODO** - rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016).
d. **Dane osobowe** - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby fizycznej.
e. **Przetwarzanie danych osobowych** - dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.
f. **Ograniczenie przetwarzania** - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
g. **Anonimizacja** - zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych.
h. **Zgoda osoby, której dane dotyczą** - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.
i. **Ocena skutków w ochronie danych** - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst

i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

j. **Podmiotem danych** jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.
k. **Odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.
l. **Podmiot przetwarzający (Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.
m. **Inspektor Ochrony Danych (IOD)** - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla Podmiotów danych i organu nadzorczego.
n. **Pseudonimizacja** - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
o. **Szczególne kategorie danych osobowych** - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życia seksualnego osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.
p. **Profilowanie** - jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
q. **Naruszenie ochrony danych osobowych** - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
r. **Zbiór danych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
s. **Personel -** pracownicy oraz wszystkie inne osoby działające w imieniu Przedsiębiorstw Holcim w Polsce, niezależnie od formy prawnej ich relacji z Holcim w Polsce.
t. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programistycznych zastosowanych w celu przetwarzania danych.
u. **Zabezpieczenie danych osobowych** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

v. **Bezpieczeństwo** - stan faktyczny uniemożliwiający przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
w. **Administrator Systemu Informatycznego (ASI)** - zespół osób upoważnionych przez Administratora, odpowiedzialny za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach.
x. **Budynki Holcim** - budynki zlokalizowane niezależnie lub w ramach biur lub zakładów Przedsiębiorstw Holcim w Polsce, aktualny wykaz adresów obiektów Holcim w Polsce jest dostępny na stronie www.holcim.pl/lokalizacje

§ 4.
Cel wprowadzenia dokumentu Polityki Bezpieczeństwa Danych Osobowych

1. Celem Polityki Bezpieczeństwa Danych Osobowych jest:
   a. osiągnięcie i utrzymanie akceptowalnego poziomu bezpieczeństwa aktywów informacyjnych Przedsiębiorstw Holcim w Polsce poprzez wdrożenie odpowiedniego systemu ochrony tych aktywów przed zagrożeniami wewnętrznymi i zewnętrznymi;
   b. zapewnienie bezpieczeństwa danym osobowym w Przedsiębiorstw Holcim w Polsce, ze szczególnym uwzględnieniem zgodności z prawem;
   c. podniesienie poziomu świadomości Personelu Przedsiębiorstw Holcim w Polsce, co do istoty problemu bezpieczeństwa danych osobowych.
2. Zarząd Przedsiębiorstw Holcim w Polsce deklaruje zaangażowanie w prawidłowe zarządzanie bezpieczeństwem danych osobowych oraz oświadcza, że dołoży wszelkich starań w celu zapewnienia bezpieczeństwa ochrony danych osobowych.

§ 5.
Zakres stosowania dokumentu Polityki Bezpieczeństwa Danych Osobowych

1. Polityka Bezpieczeństwa Danych Osobowych ma zastosowanie w stosunku do wszystkich postaci informacji zawierających dane osobowe: dokumentów papierowych, zapisów elektronicznych i innych, będących własnością Przedsiębiorstw Holcim w Polsce lub administrowanych przez Przedsiębiorstwa Holcim w Polsce i przetwarzanych w systemach informatycznych, tradycyjnych (papierowych) i komunikacyjnych Holcim w Polsce.
2. Polityka Bezpieczeństwa Danych Osobowych ma zastosowanie do całości Personelu Holcim w Polsce tj. w stosunku do wszystkich pracowników Przedsiębiorstw Holcim w Polsce, jak również osób trzecich mających dostęp do danych osobowych w Przedsiębiorstw Holcim w Polsce.
3. Ochrona danych osobowych, wynikająca z Polityki Bezpieczeństwa Danych Osobowych, jest realizowana na każdym etapie przetwarzania informacji.

§ 6.
Zasady dotyczące przetwarzania danych osobowych

Dane osobowe muszą być:

a. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ***(„zgodność z prawem, rzetelność i przejrzystość”)***;
b. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami ***(„ograniczenie celu”)***;

c. adekwatne, stosowne oraz ograniczone do tego, co jest niezbędne do celów, w których są przetwarzane ***(„minimalizacja danych”)***;
d. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ***(„prawidłowość”)***;
e. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89, ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy rozporządzenia RODO w celu ochrony praw i wolności osób, których dane dotyczą ***(„ograniczenie przechowywania”)***;
f. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ***(„integralność i poufność”)***.

§ 7.
Inspektor ochrony danych osobowych

1. **Zarząd Przedsiębiorstw Holcim w Polsce powołał Inspektora Ochrony Danych - Krzysztof Radtke.** Podlega on bezpośrednio Zarządowi Przedsiębiorstw Holcim w Polsce i wypełnia swoje zadania zgodnie z rozporządzeniem RODO.
2. Do najważniejszych obowiązków Inspektora Ochrony Danych należy:
    a. informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów prawnych o ochronie danych i doradzanie im w tej sprawie;
    b. monitorowanie przestrzegania przepisów o ochronie danych przez Administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe;
    c. zapewnienie przetwarzania danych osobowych zgodnie z uregulowaniami Polityki Bezpieczeństwa Danych Osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    d. wydawanie i anulowanie, równolegle z Administratorem, upoważnień do przetwarzania danych osobowych;
    e. prowadzenie, równolegle z Administratorem, ewidencji osób upoważnionych do przetwarzania danych osobowych;
    f. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania;
    g. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
    h. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
    i. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
    j. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
    k. współpraca z organem nadzorczym.
3. Inspektor Ochrony Danych ma prawo:

   a. rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w Przedsiębiorstwach Holcim w Polsce;
   b. wstępu do pomieszczeń, w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych, w celu oceny zgodności przetwarzania danych z przepisami prawa;
   c. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
   d. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
   e. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych, służących do przetwarzania danych.
4. Osoby, których dane dotyczą, mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO pod adresem poczty elektronicznej:

pl-m-inspektor-ochrony-danych@holcim.com

§ 8.
Ocena skutków - Analiza ryzyka

1. Ocena skutków jest formalną, określoną w art. 35 RODO, procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator.
2. Ocena skutków musi być wykonana przy współudziale Inspektora Ochrony Danych.
3. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć, a dane te w postaci zbiorów (kategorii osób) zostają wykazane w Rejestrze czynności przetwarzania (RCP), przy czym zestawienie operacji przetwarzania (inwentaryzacja aktywów) obejmuje: opis zbiorów (kategorii osób), nazwę zbioru (opis kategorii osób), opis celów przetwarzania, charakter, zakres, kontekst danych osobowych, odbiorców danych, funkcjonalny opis operacji przetwarzania, aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing).
4. Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO) obejmuje - w ramach przeprowadzenia oceny skutków (analizy ryzyka) - potwierdzenie, że Administrator (lub Podmiot przetwarzający) spełnienia obowiązki prawne wobec danych w zbiorach (dla kategorii osób) poprzez zapewnienie, że:
   a. dane te są legalnie przetwarzane (na podstawie art. 6, 9),
   b. dane te są adekwatne w stosunku do celów przetwarzania,
   c. dane te są przetwarzane przez określony czas (retencja danych),
   d. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
   e. opracowano klauzule informacyjne dla kategorii osób,
   f. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28), które są rejestrowane metodami wdrożonymi w Holcim w Poslce,
   g. potwierdzenie spełnienia powyższych wymagań prawnych RODO znajduje się w Rejestrze Czynności Przetwarzania (§ 9. p.7 lit. f. poniżej).
5. Analiza ryzyka obejmuje ustrukturyzowany zbiór zasad dla przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

6. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania (np. dla zbioru pracowników, zbioru klientów, dla procesu wysyłania informacji handlowej z bazy marketingowej).

7. W ramach analizy ryzyka stosuje się dodatkowe definicje jak niżej:
    a. **Aktywa** - środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych,
    b. **Naruszenie (Incydent) ochrony danych osobowych** - to 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,
    c. **Zagrożenie** - potencjalne naruszenie (potencjalny incydent),
    d. **Skutki** - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia),
    e. **Ryzyko** - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.
8. Przy wyznaczaniu zagrożeń:
    a. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania,
    b. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.
9. Wyliczenie ryzyka dla zagrożeń obejmuje:
    a. Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania, gdzie ustaloną skalę prawdopodobieństwa prezentuje Tabela A,
    b. Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne, gdzie ustaloną skalę Skutków prezentuje Tabela B,
    c. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły:

$$R = P \times S$$

Tabela A **Prawdopodobieństwo wystąpienia zagrożenia (P)**	**Skala (Waga)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B **Skutki wystąpienia zagrożenia**	**Skala (Waga)**
małe (do 10.000 PLN, incydent prasowy lokalny)	1
średnie (10.000 - 100.000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100.000 PLN, naruszenie prawa)	3

10. Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem obejmuje:
    a. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem,
    b. ustaloną skalę Ryzyka prezentuje Tabela C.

Tabela C Poziom ryzyka	Wartość [R = P x S]
ryzyko pomijalne i akceptowalne (akceptujemy)	1 - 2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3 - 6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

11. Reakcja na wartość ryzyka obejmuje:
    a. Akceptacja ryzyka - zabezpieczenia są właściwe - brak potrzeby stosowania dodatkowych zabezpieczeń;
    b. Działania obniżające ryzyko, które może zastosować Administrator:
        1) **Przeniesienie** - przerzucenie ryzyka (outsourcing, ubezpieczenie),
        2) **Unikanie** - eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji),
        3) **Redukcja** - zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. szyfrowanie pendrivów z danymi wynoszonych poza firmę),
    c. Analizę ryzyka przeprowadza się w ustalonym szablonie (dokumenty wewnętrzne Organizacji).
12. Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów/kategorii osób, realizacja nowych procesów przetwarzania, zmiany prawne).
13. Zarządzanie ryzykiem obejmuje także Plan postępowania z ryzykiem poprzez:
    a. wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, określając Plan postępowania z ryzykiem (dokumenty wewnętrzne Organizacji),
    b. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń**.**

§ 9.

Środki techniczne i organizacyjne niezbędne dla realizacji zasad przetwarzania danych osobowych

1. Administrator Danych Osobowych w ramach **Przedsiębiorstw Holcim w Polsce** prowadzi zarządzanie bezpieczeństwem danych osobowych poprzez proces ciągły, realizowany przy współdziałaniu użytkowników z Inspektorem Ochrony Danych oraz Administratorem Systemów Informatycznych.
2. W Przedsiębiorstwach Holcim w Polsce przy przetwarzaniu danych stosuje się środki techniczne i organizacyjne zapewniające ochronę danych, określone w art. 32-36 RODO w szczególności, zapewnia zabezpieczenie integralności i poufności danych osobowych.
3. Przedsiębiorstwa Holcim w Polsce realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznaczyły budynki, pomieszczenia i części pomieszczeń, tworzące obszary Przedsiębiorstw Holcim w Polsce, w których przetwarzane są dane osobowe.
4. Dostęp do miejsc, w których przetwarzane są dane osobowe, zabezpieczony jest poprzez system zabezpieczeń fizycznych i elektronicznych oraz nadzorowany przez Przedsiębiorstwa Holcim w Polsce.
5. Obiekty i tereny Przedsiębiorstw Holcim są chronione przez podmioty profesjonalne i/lub upoważniony personel, w sposób fizyczny i/lub elektroniczny, w tym poprzez monitoring wizyjny. Informacja o wykorzystaniu monitoringu wizyjnego znajduje się w miejscach wstępu na tereny/zakłady Przedsiębiorstw Holcim w Polsce oraz na fizycznych barierach wstępu

(np. ogrodzenia), a także w miejscach ogólnodostępnych i widocznych dla wszystkich wchodzących w obszar monitoringu wizyjnego.

6. Przedsiębiorstwa Holcim w Polsce wchodzą w skład Grupy Kapitałowej HOLCIM, z siedzibą w Szwajcarii, w ramach której zawarta jest Wewnętrz Korporacyjna Umowa Przetwarzania Danych przez Przedsiębiorstwa Holcim w Polsce oraz przez inne podmioty zrzeszone z Holcim. Lista podmiotów Grupy Kapitałowej Holcim jest dostępna w **linku.**
7. Przedsiębiorstwa Holcim w Polsce stosują także następujące rozwiązania dla zapewnienia bezpieczeństwa danych:
    a. **Upoważnienia do przetwarzania danych** - gdzie obowiązują następujące zasady:
        1) Administrator odpowiada za nadawanie/anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych.
        2) Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
        3) Upoważnienia nadawane są na wniosek przełożonych osób.
        4) Upoważnienia nadawane są w formie udokumentowanego zakresu obowiązków.
        5) Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.
        6) Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych, przy czym ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO.
    b. **Sformalizowane zasady stosowania środków organizacyjnych i technicznych zabezpieczające dane osobowe** - gdzie obowiązują następujące zasady:
        1) Administrator jest zobowiązany do stosowania środków technicznych i organizacyjnych (zabezpieczeń) adekwatnych do zagrożeń naruszenia praw i wolności osób.
        2) Administrator opracował wewnętrzne procedury zarządzania bezpieczeństwem danych i infrastrukturą, w których zabezpieczenia są opisane w zakresie wdrażania, stosowania, konserwacji i ciągłego doskonalenia.
        3) Procedury są aktualizowane, jeśli zajdzie taka potrzeba, po przeprowadzeniu analizy ryzyka/oceny skutków.
    c. **Procedura Ochrony Danych Osobowych** - gdzie obowiązują następujące zasady:
        1) Procedura (rozumiana jako zabezpieczenie) ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania.
        2) Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.
    d. **Szkolenia w zakresie ochrony danych** - dla których obowiązują następujące zasady:
        1) Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu lub zapoznana z przepisami RODO.
        2) Za przeprowadzenie szkolenia odpowiada IOD.
        3) W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych jest ono udokumentowane metodami wdrożonymi w Organizacji.

4) Po przeszkoleniu z zasad ochrony danych osobowych, uczestnik potwierdza znajomość tych zasad oraz zobowiązuje się do ich stosowania.

e. Ustrukturyzowane **zasady postępowania z incydentami**:
   1) Wewnętrzny dokument (procedura):
      a) definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie,
      b) ma na celu minimalizację skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
   2) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania bezpośredniego przełożonego (lub Inspektora Ochrony Danych) o stwierdzeniu podatności lub wystąpieniu incydentu.
   3) Do typowych podatności bezpieczeństwa danych osobowych należą:
      a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
      b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
      c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
   4) Do typowych incydentów bezpieczeństwa danych osobowych należą:
      a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
      b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
      c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome niszczenie dokumentów/danych, działanie wirusów lub innego szkodliwego oprogramowania).
   5) W przypadku stwierdzenia wystąpienia incydentu IOD prowadzi postępowanie wyjaśniające w toku, którego:
      a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
      b) inicjuje ewentualne działania dyscyplinarne,
      c) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
      d) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
   6) Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
   7) Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
   8) W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu.

9) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki powiadamia osobę, której dane dotyczą, o takim naruszeniu.

f. **Rejestr czynności przetwarzania** - gdzie obowiązują następujące zasady:
   1) Administrator prowadzi rejestr w formie udokumentowanej,
   2) podmiot przetwarzający także prowadzi rejestr w formie udokumentowanej.

g. **Audyty** - gdzie obowiązują następujące zasady:
   1) zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania,
   2) w tym celu Administrator stosuje sformalizowane zasady dot. audytów,
   3) w celu udokumentowania przeprowadzenia audytu, Administrator wykorzystuje określone wewnętrznie zasady.

h. **Zasady przywrócenia dostępności danych osobowych i dostępu do nich** w razie incydentu fizycznego lub technicznego (BCP):
   1) zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
   2) Administrator opracował procedury przywracania, które są dokumentami wewnętrznymi Organizacji.

§ 10.
Prawa osób, których dane są przetwarzane przez Holcim w Polsce

1. Przedsiębiorstwa Holcim w Polsce gwarantują osobom fizycznym, których dane osobowe są przetwarzane w związku z bieżącą działalnością, realizację uprawnień przyznanych im przez obowiązujące przepisy prawa.
2. W szczególności każdej osobie fizycznej, której dane osobowe są przetwarzane w związku z działalnością Przedsiębiorstw Holcim w Polsce, przysługuje prawo do żądania od Administratora dostępu do jej danych osobowych, do ich sprostowania, usunięcia lub ograniczenia przetwarzania lub prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.

§ 11.
Konsekwencje naruszenia Polityki Bezpieczeństwa Danych Osobowych

Osoby naruszające zasady Polityki Bezpieczeństwa Danych Osobowych zostaną pociągnięte do odpowiedzialności służbowej (porządkowej lub dyscyplinarnej) lub karnej.

§ 12.
Postanowienia końcowe

1. Szczegółowe zasady dotyczące przetwarzania danych osobowych uregulowane zostały w procedurach i instrukcjach o charakterze wewnętrznym.
2. Niniejsza Polityka zastępuje w całości wydanie z 1.06.2023 r. i podlega publikacji w wewnętrznych i zewnętrznych kanałach komunikacji Przedsiębiorstw Holcim w Polsce, w tym na stronie www.holcim.pl .

Xavier Guesnu

Prezes Zarządu
Przedsiębiorstw Holcim w Polsce

(dokument podpisany elektronicznie)