Uchwała nr 20/R/16
Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa
z dnia 22 września 2016 roku
w sprawie zatwierdzenia uchwał Prezydium Rady
Łódzkiej Okręgowej Izby Inżynierów Budownictwa.

§ 1

Na podstawie art. 19 ust. 1 pkt 1 ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (*tekst jednolity Dz.U. z 2014 r., poz. 1946 z późn. zm.*), § 5 ust. 2 Regulaminu okręgowych rad Polskiej Izby Inżynierów Budownictwa (*ost. popr. i uzup. Uchwałą II Nadzwyczajnego Krajowego Zjazdu PIIB nr 14/15 z dnia 20 sierpnia 2015 r.*), oraz art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity Dz. U. z 2016 r., poz. 922*) oraz § 1 pkt 1, § 3-5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.*) Okręgowa Rada Łódzkiej Okręgowej Izby Inżynierów Budownictwa zatwierdza podjętą przez Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa uchwałę Nr 6/PR/16 z dnia 28 lipca 2016 r. w sprawie przyjęcia Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych Łódzkiej Okręgowej Izby Inżynierów Budownictwa.

§ 2

Na podstawie art. 19 ust. 1 pkt 1 ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (*tekst jednolity Dz.U. z 2014 r., poz. 1946 z późn. zm.*), § 5 ust. 2 Regulaminu okręgowych rad Polskiej Izby Inżynierów Budownictwa (*ost. popr. i uzup. Uchwałą II Nadzwyczajnego Krajowego Zjazdu PIIB nr 14/15 z dnia 20 sierpnia 2015 r.*), Okręgowa Rada Łódzkiej Okręgowej Izby Inżynierów Budownictwa zatwierdza podjęte przez Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa uchwały:

1) Nr 7/PR/16 z dnia 28 lipca 2016 r. w sprawie przyznania odznak honorowych PIIB;
2) Nr 8/PR/16 z dnia 8 września 2016 r. w sprawie przyznania zapomóg;
3) Nr 9/PR/16 z dnia 8 września 2016 r. w sprawie przyznania dofinansowania.

§ 3

Uchwała wchodzi w życie w dniu podjęcia. Postanowienia Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemami Informatycznymi Służącymi Do Przetwarzania Danych Osobowych Łódzkiej Okręgowej Izby Inżynierów Budownictwa obowiązują od dnia 1 października 2016 r.

Załączniki:

1) uchwała Nr 6/PR/16 z dnia 28 lipca 2016 r. wraz z załącznikami;
2) uchwała Nr 7/PR/16 z dnia 28 lipca 2016 r. wraz z załącznikami;
3) uchwała Nr 8/PR/16 z dnia 8 września 2016 r.;
4) uchwała Nr 9/PR/16 z dnia 8 września 2016 r.

Sekretarz Rady ŁOIIB — Przewodnicząca Rady ŁOIIB

mgr inż. Grzegorz Rakowski — mgr inż. Barbara Malec

Uchwała Nr 6/PR/16

Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa

z dnia 28 lipca 2016 r.

w sprawie przyjęcia Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych Łódzkiej Okręgowej Izby Inżynierów Budownictwa.

§ 1

Na podstawie § 5 ust. 1 pkt 5 Regulaminu okręgowych rad Polskiej Izby Inżynierów Budownictwa uchwalonego w dniu 27 września 2002 r. przez I Krajowy Zjazd Polskiej Izby Inżynierów Budownictwa (*ost. popr. i uzup. Uchwałą II Nadzwyczajnego Krajowego Zjazd PIIB nr 14/15 z dnia 20 sierpnia 2015 r.*) oraz art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity Dz. U. z 2016 r., poz. 922*), Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa przyjmuje Politykę Bezpieczeństwa oraz Instrukcję Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych Łódzkiej Okręgowej Izby Inżynierów Budownictwa. Polityka Bezpieczeństwa stanowi załącznik nr 1 do niniejszej uchwały. Instrukcję Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych stanowi załącznik nr 2 do niniejszej uchwały.

§ 2

Zgodnie z § 5 ust. 2 ww. Regulaminu okręgowych rad Polskiej Izby Inżynierów Budownictwa niniejsza uchwała wymaga przedstawiania do zatwierdzenia Okręgowej Radzie na jej najbliższym posiedzeniu.

§ 3

Uchwała wchodzi w życie w dniu podjęcia, przy czym Polityka Bezpieczeństwa oraz Instrukcja Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych obowiązują od dnia 1 października 2016 r.

Załączniki:

1) Polityka bezpieczeństwa.
2) Instrukcja Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych

Sekretarz Rady ŁOIIB

mgr inż. Grzegorz Rakowski

Przewodnicząca Rady ŁOIIB

mgr inż. Barbara Malec

POLITYKA BEZPIECZEŃSTWA

ŁÓDZKA OKRĘGOWA IZBA INŻYNIERÓW BUDOWNICTWA

www.lod.piib.org.pl

91-425 ŁÓDŹ

Ul. PÓŁNOCNA 39

NIP: 725-18-49-050

SPIS TREŚCI

INFORMACJE OGÓLNE.

Łódzka Okręgowa Izba Inżynierów Budownictwa, zwana dalej Izbą, jako jednostka organizacyjna samorządu zawodowego inżynierów budownictwa uznaje ochronę danych osobowych członków okręgowej izby oraz innych osób za podstawowy cel działania organów i biura okręgowej izby.

Izba, będąc Administratorem Danych, opracowała niniejszy dokument Polityka Bezpieczeństwa, w celu zapewnienia zgodności przetwarzania danych osobowych z polskim ustawodawstwem.

Polityka Bezpieczeństwa wraz z Instrukcją Zarządzania Systemem Informatycznym Służącymi Do Przetwarzania Danych Osobowych stanowi dokumentację przetwarzania danych osobowych w rozumieniu art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity Dz. U. z 2016 r., poz. 922*) oraz § 1 pkt 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.*).

Niniejsza Polityka Bezpieczeństwa obowiązuje od dnia 1 października 2016 r. Wszelkie wątpliwości dotyczące sposobu interpretacji postanowień niniejszego dokumentu Polityki Bezpieczeństwa, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Każda osoba mającą dostęp do danych osobowych z upoważnienia Administratora Danych, została zapoznana z Polityką Bezpieczeństwa i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych oraz członków organów Izby. Osoby o których mowa, złożyły na piśmie oświadczenie o zapoznaniu się z treścią Polityki Bezpieczeństwa oraz zobowiązały się do stosowania zawartych w niej postanowień.

CEL PRZYGOTOWANIA POLITYKI BEZPIECZEŃSTWA.

Podstawowym celem przyświecającym przygotowaniu i wdrożeniu dokumentu Polityki Bezpieczeństwa jest zapewnienie zgodności działania Izby i jej organów z ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi. Dokument Polityki Bezpieczeństwa został opracowany na podstawie przepisów zawartych w następujących aktach prawnych:

1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity Dz. U. z 2016 r., poz. 922*),
2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.*),
3) ustawa z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (*tekst jednolity Dz. U. z 2014 r., poz. 1946 z późn. zm.*),
4) Statut Polskiej Izby Inżynierów Budownictwa (w brzmieniu ustalonym *Uchwałą II. Nadzwyczajnego Krajowego Zjazdu Polskiej Izby Inżynierów Nr 8/15 z dnia 20 sierpnia 2015 r. zmieniająca uchwałę w sprawie uchwalenia statutu Polskiej Izby Inżynierów Budownictwa*),
5) Regulamin okręgowych rad Polskiej Izby Inżynierów Budownictwa (w brzmieniu ustalonym *Uchwałą II. Nadzwyczajnego Krajowego Zjazdu Polskiej Izby Inżynierów Nr 14/15 z dnia 20 sierpnia 2015 r. zmieniająca uchwałę w sprawie regulaminu okręgowych rad Polskiej Izby Inżynierów Budownictwa*).

Należy przez powyższe rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zadaniem Polityki Bezpieczeństwa jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ICH STOSOWANIA.

Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Izby. Polityka Bezpieczeństwa, odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemie informatycznym. Na Politykę Bezpieczeństwa zgodnie z § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.*), składają się następujące informacje:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
4) sposób przepływu danych pomiędzy poszczególnymi systemami,
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Politykę Bezpieczeństwa stosuje się do wszelkich czynności, stanowiących w myśl ustawy o ochronie danych osobowych, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady przetwarzania danych osobowych ujęte w niniejszym dokumencie Polityki Bezpieczeństwa.

WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKA BEZPIECZEŃSTWA.

1) **administrator danych** - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych, tj. Łódzką Okręgową Izbę Inżynierów Budownictwa, zwaną dalej „Izbą",
2) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3) **hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
4) **identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
5) **instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych** – dokument instrukcji zarządzania systemem informatycznym w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „instrukcją",
6) **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
7) **odbiorca danych** - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby upoważnionej do przetwarzania danych,
    c) przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
    d) podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
    e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
8) **państwo trzecie** - rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego,
9) **Polityka Bezpieczeństwa** – dokument Polityki Bezpieczeństwa w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „Polityką",
10) **poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

11) **przetwarzanie danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym,
12) **raport** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
13) **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
14) **rozporządzenie** – rozumie się przez to rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.*), zwane dalej „rozporządzeniem",
15) **sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (*Dz. U. z 2000 r., Nr 73, poz. 852 z późn. zm.*) i publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne (*tekst jednolity Dz. U. z 2014 r., poz. 243 z późn. zm.*),
16) **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (*Dz. U. z 2000 r., Nr 73, poz. 852 z późn. zm.*) i sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne (*tekst jednolity Dz. U. z 2014 r., poz. 243 z późn. zm.*),
17) **system informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
18) **teletransmisja** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
19) **ustawa** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity Dz. U. z 2016 r., poz. 922*), zwaną dalej „ustawą",
20) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

21) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

22) **zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

23) **zbiór danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

24) **zgoda osoby, której dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH.

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych odpowiadają:

1) Administrator Danych,
2) Administrator Systemu Informatycznego,
3) Każda osoba wykonująca pracę bądź świadcząca usługi na rzecz Izby, która uzyskała upoważnienie do przetwarzania danych osobowych.

ADMINISTRATOR DANYCH.

Łódzka Okręgowa Izba Inżynierów Budownictwa z siedzibą: ul. Północna 39, 91-425 Łódź, działająca na podstawie ustawa z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (*tekst jednolity Dz. U. z 2014 r., poz. 1946 z późn. zm.*), wpisana do Krajowego Rejestru Urzędowego Podmiotów Gospodarki Narodowej pod numerem REGON 473043690, identyfikująca się numerem NIP 725-18-49-050 jest Administratorem Danych.

W imieniu Administratora Danych obowiązki określone w Ustawie i Rozporządzeniu pełni Okręgowa Rada w imieniu której działa Przewodnicząca Okręgowej Rady oraz Prezydium Okręgowej Rady.

Na dzień wejścia w życie Polityki Bezpieczeństwa funkcje te pełnią następujące osoby:

1) Barbara Malec - Przewodnicząca Okręgowej Rady;
2) Piotr Parkitny - Zastępca Przewodniczącej;
3) Agnieszka Jońca - Zastępca Przewodniczącej;
4) Grzegorz Rakowski - Sekretarz;
5) Cezary Wójcik - Skarbnik;
6) Jan Wójt - Zastępca Sekretarza;
7) Urszula Jakubowska - Zastępca Skarbnika;
8) Danuta Ulańska - Członek Prezydium;
9) Bogdan Krawczyk - Członek Prezydium;
10) Sławomir Najgiebauer - Członek Prezydium.

Zmiana osób pełniących funkcję Przewodnicząca Okręgowej Rady oraz Prezydium Okręgowej Rady nie wymaga zmiany Polityki Bezpieczeństwa.

Zgodnie z ustawą z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (*tekst jednolity Dz. U. z 2014 r., poz. 1946 z późn. zm.*) organami Łódzkiej Okręgowej Izby Inżynierów Budownictwa są:

1) Okręgowy Zjazd Izby;
2) Okręgowa Rada Izby;
3) Okręgowa Komisja Rewizyjna;
4) Okręgowa Komisja Kwalifikacyjna;

5) Okręgowy Sąd Dyscyplinarny;

6) Okręgowy Rzecznik Odpowiedzialności Zawodowej.

Szczegółowe kompetencje poszczególnych organów, ich przewodniczących oraz członków określają przepisy ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa, rozporządzeń wydanych na podstawie wymienionej ustawy, jak również przepisy ustawy z dnia 7 lipca 1994 r. Prawo budowlane (*tekst jednolity Dz.U. z 2016 r., poz. 290 z późn. zm.*). Kompetencje poszczególnych organów określone zostały również w Statucie Polskiej Izby Inżynierów Budownictwa oraz regulaminach wydanych na podstawie ww. przepisów ustawowych.

Każdy członek ww. organów jest zobowiązany jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych oraz do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu pełnienia funkcji w organie.

Członek organu posiada dostęp do określonego zbioru danych osobowych tylko w sytuacji, gdy przewidują to ww. przepisy lub regulaminy i wyłącznie w zakresie, w jakim wynika to z przywołanych uregulowań. W przypadkach, gdy brak jest regulacji, z których jednoznacznie wynika, że członek organu może przetwarzać dane osobowe lub członek organu ma przetwarzać dane osobowe poza zakresem określonym w wymienionych uregulowaniach konieczne jest uzyskanie pisemnego upoważnienia, otrzymanego w trybie określonym w Rozdziale „Upoważnienia do przetwarzania danych osobowych", zapisy dotyczące uzyskiwania upoważnienia przez pracowników stosuje się odpowiednio.

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO.

Funkcję Administratora Systemu Informatycznego pełni osoba wskazana pisemnie przez Administratora Danych. Powierzenie funkcji Administratora Systemu Informatycznego określonej osobie wynika z zawartej umowy cywilnoprawnej albo umowy o pracę.

Zmiana osoby pełniącej funkcję Administratora Systemu Informatycznego następuje na skutek decyzji Administratora Danych.

W przypadku odwołania lub rezygnacji ze stanowiska Administratora Systemu Informatycznego, Administrator Danych niezwłocznie wyznacza na to stanowisko inną osobę.

Do uprawnień i obowiązków Administratora Systemu Informatycznego należą, w szczególności:

a) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemie informatycznym,
b) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemie informatycznym, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tego systemu,
c) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
d) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemie informatycznym i tradycyjnych,
e) sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi opisanymi w Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych,
f) inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemem informatycznym, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
g) podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemie informatycznym, o których mowa w Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych,
h) informowanie Administratora Danych o konieczności wprowadzenia zmian w Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych wraz ze wskazaniem przyczyn wprowadzenia zmian.

PRACOWNICY BIURA ŁÓDZKIEJ OKRĘGOWEJ IZBY INŻYNIERÓW BUDOWNICTWA.

Każdy pracownik Izby, który uzyskał upoważnienie do przetwarzania danych osobowych, zobowiązany jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych.

Dostęp do określonego zbioru danych osobowych pracownik Izby uzyskuje na podstawie pisemnego upoważnienia, otrzymanego w trybie określonym w Rozdziale „Upoważnienia do przetwarzania danych osobowych", niniejszej Polityki Bezpieczeństwa.

Pracownicy zatrudnieni - na podstawie umowy o pracę, bądź osoby świadczące usługi na podstawie umów cywilnoprawnych - przy przetwarzaniu danych osobowych zobowiązani są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia lub rozwiązaniu umowy. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w Załączniku nr 1.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH.

1. Izba realizując niniejszą Politykę Bezpieczeństwa, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie pracownikom, którzy uzyskali uprzednie, stosowne upoważnienie do przetwarzania danych osobowych, nadawane przez Przewodnicząca Okręgowej Rady lub osoby ją zastępujące.
2. Upoważnienie do przetwarzania danych osobowych mogą uzyskać wyłącznie pracownicy Izby.
3. Dostęp do danych osobowych i ich przetwarzania bez odrębnego upoważnienia, o którym mowa w niniejszym Rozdziale może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa.
4. W szczególności dostęp do danych osobowych na podstawie zasady określonej w pkt. 3 posiadają: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Agencja Bezpieczeństwa Wewnętrznego, sądy powszechne, Najwyższa Izba Kontroli, Generalny Inspektor Ochrony Danych Osobowych, podmioty którym powierzono przetwarzanie danych osobowych oraz inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień – wszystkie ww. po okazaniu dokumentów potwierdzających te uprawnienia.
5. Upoważnienie, o którym mowa w niniejszym Rozdziale, wydawane jest każdemu z pracowników osobno, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.
6. Wzór upoważnienia stanowi Załącznik nr 1 do Polityki Bezpieczeństwa.
7. Upoważnienia wydawane są zgodnie z następującą procedurą:
   1) Dyrektor Biura, Przewodniczący Organu Izby lub Dział kadr informują Przewodniczącą Okręgowej Rady o konieczności nadania pracownikowi upoważnienia do przetwarzania danych osobowych w określonych zbiorach.
   2) Dyrektor Biura Izby przed nadaniem pracownikowi upoważnienia, organizuje dla niego krótkie szkolenie, podczas którego osoba jest informowana o podstawowych aspektach prawnych związanych z ochroną danych osobowych (najważniejsze definicje, odpowiedzialność prawna, obowiązek właściwego zabezpieczenia danych przetwarzanych w formie papierowej oraz w systemie informatycznym). Szkolenie może zostać przeprowadzone w następującej formie:
   a) osobiście bądź wyznaczoną przez niego osobę w siedzibie Izby;

b) w formie e-learningu za pośrednictwem internetowej platformy szkoleniowej. Pracownik po otrzymaniu loginu i hasła do platformy uczestniczy w szkoleniu samodzielnie. Szkolenie zostanie zakończone w momencie, kiedy wiedza pracownika z zakresu ochrony danych osobowych zostanie zweryfikowana pomyślnie za pomocą testu.

3) Przewodnicząca Okręgowej Rady sporządza upoważnienie dla pracownika, który wykaże, że odbył i pomyślnie ukończył szkolenie.
4) Z obowiązku szkolenia zwolnione są osoby, które wykażą właściwymi dokumentami, iż posiadają odpowiednie wykształcenie z zakresu ochrony danych osobowych.
5) Poza szkoleniem, którego odbycie warunkuje uzyskanie uprawnień do nadania pracownikowi upoważnienia do przetwarzania danych osobowych, dodatkowo będą odbywały się cykliczne szkolenia dotyczące doskonalenia i utrwalania wiedzy z zakresu ochrony danych osobowych dla pracowników Izby.
6) Upoważnienie jest drukowane w dwóch egzemplarzach, z których każdy musi być podpisany przez pracownika któremu nadano upoważnienie.
7) Jeden egzemplarz upoważnienia jest przechowywany jako część dokumentacji kadrowej, drugi jest wydawany pracownikowi, któremu nadano upoważnienie.

8. Wydanie każdego upoważnienia jest odnotowywane przez Dyrektora Biura Izby w prowadzonej i nadzorowanej przez niego elektronicznej ewidencji upoważnień we wszystkich zbiorach danych osobowych oraz przez dział kadr w papierowej ewidencji upoważnień która stanowi Załącznik nr 2 do niniejszej Polityki Bezpieczeństwa.
9. W przypadku stwierdzenia, iż dany pracownik uzyskał zbyt szerokie uprawnienia w zakresie przetwarzania danych osobowych, nieuzasadnione wykonywanymi przez niego zadaniami służbowymi lub innymi obowiązkami o charakterze merytorycznym, oraz gdy było to przyczyną naruszenia poziomu bezpieczeństwa przetwarzania danych osobowych niezwłocznie Przewodnicząca Okręgowej Rady cofa lub zmienia upoważnienie.
10. Zakres nadanych pracownikowi uprawnień może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez niego określonych zadań w określonym przedziale czasu. W takim przypadku tryb wskazany do nadawania uprawnień określony w przedmiotowym Rozdziale jest właściwy również w razie zmiany zakresu uprawnień pracownika w związku z jego dostępem do określonego zbioru danych osobowych.

11. W przypadku zaistnienia konieczności cofnięcia upoważnienia do przetwarzania danych osobowych, informuje się o tym Przewodniczącą Okręgowej Rady, Dyrektora Biura Izby oraz dział kadr w celu aktualizacji ewidencji upoważnień.
12. Utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:
    1) zmiany stanowiska pracy w Izbie 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 w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,
    2) umyślnego naruszenia zasad ochrony danych osobowych określonych w Ustawie, Rozporządzeniu, Polityce Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych,
    3) rozwiązania stosunku pracy,
    4) rozwiązania umowy cywilnoprawnej,
    5) aktualizacji wzoru upoważnienia, w takim przypadku wszystkim pracownikom którzy byli do tej pory upoważnieni do przetwarzania danych osobowych, niezwłocznie wydawane są nowe upoważnienia zgodnie z procedurą opisaną w pkt. 7 niniejszego Rozdziału.
13. Uszczegółowienie trybu nadania, zmiany, utraty uprawnień logicznego dostępu do danych osobowych przetwarzanych w systemie informatycznym zawiera Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH OSOBOWYCH.

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   1) nieuprawniony dostęp lub próbę dostępu do systemu lub pomieszczeń w których następuje proces przetwarzania danych (widoczne uszkodzenia bądź naruszenia zabezpieczeń);
   2) naruszenie lub próbę naruszenia zbioru danych oraz integralności systemu;
   3) nieautoryzowane zniszczenie lub próbę zniszczenia danych zgromadzonych w zbiorach papierowych oraz systemie;
   4) zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany; nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);
   5) inny stan systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem.
2. Instrukcję stosuje się odpowiednio w przypadku stwierdzenia, że stan dokumentacji lub stan pomieszczeń bądź szaf biurowych, w których przechowywana jest dokumentacja wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby nieupoważnione.
3. W przypadku stwierdzenia naruszenia danych w systemie informatycznym lub zaistnienia okoliczności wskazujących na naruszenie zabezpieczeń systemu informatycznego, w którym przetwarzane są dane osobowe, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Dyrektora Biura Izby i Administratora Systemu Informatycznego.
4. Do czasu przybycia osób wskazanych w ust. 3, użytkownik:
   1) zabezpiecza dostęp do miejsca lub urządzenia;
   2) wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane;
   3) podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
5. Dyrektor Biura Izby lub Administrator Systemu Informatycznego po przybyciu na miejsce, w którym doszło do naruszenia ochrony danych osobowych:

1) ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe, stan urządzeń i zbioru danych;
2) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, odłączenie wadliwych urządzeń, zmiana haseł, blokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych);
3) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia, jak również sprawdza zawartość zbioru danych osobowych;
4) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych;
5) sprawdza sposób działania programu (w tym również obecność wirusów komputerowych);
6) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu;
7) niezwłocznie zapewnia przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia baz danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności;
8) sprawdza jakość komunikacji w systemie informatycznym;
9) dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych wskutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych;
10) spisuje relację osoby zatrudnionej przy przetwarzaniu danych, która dokonała powiadomienia;
11) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych i w przypadkach uzasadnionych niezwłocznie powiadamia Przewodniczącą Okręgowej Rady lub Prezydium Okręgowej Rady;
12) sporządza szczegółowy raport zawierający w szczególności: dane personalne osoby, która stwierdziła naruszenie, datę i godzinę powiadomienia, opis podjętych czynności i ich uzasadnienie.

6. Raport, o którym mowa w ust. 3 pkt 12 przekazywany jest bezzwłocznie Przewodniczącej Okręgowej Rady i w zależności od potrzeb innym organom Izby;
7. Ponowne uruchomienie komputerów i innych urządzeń oraz kontynuowanie pracy w systemie następuje po wydaniu opinii przez Administrator Systemu Informatycznego.

8. Dokonywanie zmian w miejscu naruszenia ochrony bez uzyskania zgody, o której mowa w ust. 5 jest dopuszczalne, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.
9. Dyrektor Biura Izby podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

1) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcę usług telekomunikacyjnych;
2) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje o ich ukaranie w trybie przewidzianym odrębnymi przepisami.

UMOWY POWIERZENIA DANYCH OSOBOWYCH.

1. Izba realizując niniejszą Politykę Bezpieczeństwa dopuszcza, by dane osobowe których jest administratorem, były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danego zbioru w określonym celu i zakresie podmiotowi zewnętrznemu na mocy umowy powierzenia przetwarzania danych osobowych.
2. Pisemna umowa powierzenia przetwarzania danych osobowych, o której mowa w niniejszym Rozdziale musi być zgodna z postanowieniami art. 31 ustawy o ochronie danych osobowych.
3. Powierzenia przetwarzania danych osobowych zgodnie z przepisami ustawy o samorządach zawodowych architektów oraz inżynierów budownictwa można dokonać na podstawie oświadczenia woli w formie uchwały Okręgowej Rady zatwierdzającej umowę. Powierzenie przetwarzania danych osobowych może nastąpić na podstawie pisemnej umowy, aneksu do umowy lub klauzuli do umowy.
4. W przypadku, gdy powierzenie danych osobowych wynika wprost z zawartej z danym podmiotem umowy, nie ma konieczności sporządzania dodatkowo pisemnej umowy powierzenia danych osobowych.
5. Każdorazowe dokonanie powierzenia danych osobowych o którym mowa w niniejszym Rozdziale musi obligatoryjnie zostać odnotowane w Polityce Bezpieczeństwa.
6. Od powierzenia danych na podstawie ww. postanowień należy odróżnić eksport danych do Polskiej Izby Inżynierów Budownictwa związanych z listą członków i kandydatów prowadzoną przez Krajową Radę Polskiej Izby Inżynierów Budownictwa.

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH.

Lp.	Nazwa zbioru danych.	Programy stosowane do przetwarzania danych osobowych w zbiorze	Uwagi
1	Rejestr członków Izby, w tym Rejestr osób ukaranych z tytułu odpowiedzialności dyscyplinarnej i Rejestr osób ukaranych z tytułu odpowiedzialności zawodowej	Członkowie ŁOIIB	Rejestr członków Izby prowadzony jest na podstawie art. 19 ust. 1 pkt 8 ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa. Obejmuje dane osobowe członków Izby, w szczególności dane związane z członkostwem w samorządzie zawodowym (status członkowski, odznaczenia samorządowe, przyznaną samopomoc i dofinansowanie szkoleń). Rejestr obejmuje również dane związane z ukaraniem członka Izba w toku postępowań prowadzonych przez organy samorządu w sprawach odpowiedzialności zawodowej i w sprawach dyscyplinarnej. Rejestr osób ukaranych z tytułu odpowiedzialności dyscyplinarnej prowadzony jest na podstawie art. 19 ust. 1 pkt 10 ww. ustawy o samorządach zawodowych architektów oraz inżynierów budownictwa, a Rejestr osób ukaranych z tytułu odpowiedzialności zawodowej na podstawie § 2 pkt 12 Regulaminu okręgowy rad Polskiej Izby Inżynierów Budownictwa, przyjętego zgodnie z art. 31 pkt 5 ww. ustawy.
2	Rejestr potencjalnych członków Izby	Członkowie ŁOIIB	Rejestr kandydatów na członków okręgowej Izby, przy czym są to wyłącznie osoby posiadające już uprawnienia budowlane. Rejestr prowadzony w związku z postępowaniami o wpisanie na listę członków okręgowej Izby opisanymi w art. 19 ust. 2 ww. ustawy o samorządach zawodowych architektów oraz inżynierów budownictwa.
3	Dziennik Korespondencji Izby	Dziennik Korespondencji v 1.0	Dziennik zawierający chronologicznie udokumentowaną korespondencję kierowaną do i przez wszystkie organy Izby oraz korespondencję wewnętrznej pomiędzy organami Izby.
4	Dziennik	Microsoft Excel część	Dziennik zawierający chronologicznie

	Korespondencji Okręgowej Komisji Kwalifikacyjnej	Microsoft Office	udokumentowaną korespondencję kierowaną do i przez Okręgową Komisję Kwalifikacyjną oraz korespondencję wewnętrzną pomiędzy Komisją a innymi organami Izby.
5	Dziennik Korespondencji Okręgowego Sądu Dyscyplinarnego	Microsoft Excel część Microsoft Office	Dziennik zawierający chronologicznie udokumentowaną korespondencję kierowaną do i przez Okręgowy Sąd Dyscyplinarny oraz korespondencję wewnętrzną pomiędzy Sądem a innymi organami Izby.
6	Dziennik Korespondencji Okręgowego Rzecznika Odpowiedzialności Zawodowej	Microsoft Excel część Microsoft Office	Dziennik zawierający chronologicznie udokumentowaną korespondencję kierowaną do i przez Okręgowego Rzecznika Odpowiedzialności Zawodowej oraz korespondencję wewnętrzną pomiędzy Rzecznikiem a innymi organami Izby.
7	Rejestr egzaminacyjny	Microsoft Access część Microsoft Office	Zbiór danych osobowych osób ubiegających się przed Okręgową Komisją Kwalifikacyjną o nadanie uprawnień budowlanych prowadzony dla poszczególnych sesji egzaminacyjnych.
8	Rejestr spraw Okręgowego Sądu Dyscyplinarnego	Microsoft Excel część Microsoft Office	Rejestr (repetytorium) postępowań w sprawach: zawodowych, dyscyplinarnych i zatarcia kary prowadzonych przez Okręgowy Sąd Dyscyplinarny dla danego roku, obejmujący wybrane dane stron postępowań.
9	Rejestr spraw Okręgowego Rzecznika Odpowiedzialności Zawodowej	Microsoft Excel część Microsoft Office	Rejestr (repetytorium) postępowań wyjaśniających w sprawach odpowiedzialności zawodowej i dyscyplinarnej prowadzonych przez Okręgowego Rzecznika Odpowiedzialności Zawodowej dla danego roku, obejmujący wybrane dane stron postępowań.
10	Rejestr kadrowo-płacowy	System enova365 oprogramowanie dla firm Zarządzenie i Księgowość	Dane osobowe pracowników i kontrahentów Izby gromadzone dla celów rozliczeniowych, w tym regulowania zobowiązań wobec ZUS i organów podatkowych.

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA POMIĘDZY NIMI.

Lp.	Nazwa zbioru danych.	Zakres przetwarzania danych.
1	**Rejestr członków Izby, w tym Rejestr osób ukaranych z tytułu odpowiedzialności dyscyplinarnej i Rejestr osób ukaranych z tytułu odpowiedzialności zawodowej**	W zbiorze przetwarzane są dane osobowe w następujących zakresach: a) „Dane osobowe" – imiona, nazwisko, data urodzenia, miejsce urodzenia, PESEL, imię ojca, imię matki, nazwisko rodowe, obywatelstwo, tytuł zawodowy; b) „Adresy" – adres zamieszkania (kod pocztowy, miejscowość, ulica, numer domu/mieszkania), adres zameldowania (kod pocztowy, miejscowość, ulica, numer domu/mieszkania), adres miejsca pracy (kod pocztowy, miejscowość, ulica, numer domu/mieszkania), email; c) „Telefony" – numer telefonu stacjonarnego, numer telefonu komórkowego i numer telefonu do miejsca pracy; d) „Dane członkowskie" – numer ewidencyjny (numer wpisu osoby na listę członków okręgowej izby), numer wniosku o wpis, data złożenia wniosku o wpisanie na listę członków, numer uchwały o wpisaniu na listę członków, data uchwały o wpisaniu na listę członków, data wpisu na listę członków, numer konta bankowego do wpłaty składki członkowskiej na okręgową izbę, numer konta bankowego do wpłaty składki członkowskiej na krajową izbę, obwód wyborczy, status członkowski; e) „Uprawnienia budowlane" – numer i data wydania decyzji o nadaniu uprawnień budowlanych, specjalność, rodzaj i zakres uprawnień budowlanych; f) „Finanse" – kwota i data wpłaty na konto bankowego do wpłaty składki członkowskiej na krajową izbę albo okręgową izbę, tytuł wpłaty; g) „Zaświadczenia" – data początkowo ważności zaświadczenia, data końcowa ważności zaświadczenia, kod weryfikacyjny zaświadczenia, data wygenerowania zaświadczenia; h) „Zawieszenia i skreślenia" – numer i data podjęcia uchwały, rodzaj uchwały (zawieszenie/skreślenie), informacja o długu wobec okręgowej izby i krajowej izby z tytułu składek członkowskich; i) „Ubezpieczenia" – informacja o obowiązkowym ubezpieczeniu z tytułu odpowiedzialności cywilnej za szkody, które mogą wyniknąć w związku z wykonywaniem samodzielnych funkcji technicznych w budownictwie w postaci nazwy ubezpieczyciela, daty obowiązywania ubezpieczenia, zakresu ubezpieczenia; j) „Dofinansowanie" – numer i data złożenia wniosku o dofinansowanie, numer i data podjęcia uchwały o dofinansowaniu, kwota dofinansowania i data jej wypłacenia, opis przyczyn dofinansowania; k) „Pełnione funkcje w ŁOIIB" – okres sprawowania funkcji, funkcja; l) „Odznaczenia" – data odznaczenia, rodzaj odznaczenia; m) „Zapomogi" - numer i data złożenia wniosku o zapomogę, numer i data podjęcia uchwały o przyznaniu zapomogi, kwota zapomogi i data jej wypłacenia, uzasadnienie przyznania zapomogi; n) „Kary" (stanowi Rejestr osób ukaranych z tytułu odpowiedzialności dyscyplinarnej i Rejestr osób ukaranych z tytułu odpowiedzialności zawodowej) – numer i data wydania decyzji przez okręgowy sąd dyscyplinarny, rodzaj kary, numer sprawy (sygn. akt), numer i data

		wydania decyzji przez krajowy sąd dyscyplinarny, data uprawomocnienia się decyzji o ukaraniu i data przekazania decyzji okręgowej radzie.
2	**Rejestr potencjalnych członków Izby**	W zbiorze przetwarzane są dane osobowe w następujących zakresach: a) „Dane osobowe" – imiona, nazwisko, data urodzenia, miejsce urodzenia, PESEL, imię ojca, imię matki, nazwisko rodowe, obywatelstwo, tytuł zawodowy; b) „Adresy" – adres zamieszkania (kod pocztowy, miejscowość, ulica, numer domu/mieszkania), adres zameldowania (kod pocztowy, miejscowość, ulica, numer domu/mieszkania), adres miejsca pracy (kod pocztowy, miejscowość, ulica, numer domu/mieszkania), email; c) „Telefony" – numer telefonu stacjonarnego, numer telefonu komórkowego i numer telefonu do miejsca pracy; d) „Dane członkowskie" – numer ewidencyjny (numer, pod jakim osoba ewentualnie zostanie wpisana na listę członków okręgowej izby), numer wniosku o wpis, data złożenia wniosku o wpisanie na listę członków, numer konta bankowego do wpłaty składki członkowskiej na okręgową izbę i składki wpisowej, , numer konta bankowego do wpłaty składki członkowskiej na krajową izbę, obwód wyborczy, status członkowski - kandydat; e) „Uprawnienia budowlane" – numer i data wydania decyzji o nadaniu uprawnień budowlanych, specjalność, rodzaj i zakres uprawnień budowlanych;
3	**Dziennik Korespondencji Izby**	W zbiorze przetwarzane są dane osobowe: nadawca (imię i nazwisko), data złożenia (wpływu korespondencji), numer korespondencji na dzienniku, adresat, dekretacja – wskazanie osoby lub organu do której kierowana jest korespondencja, do wiadomości – dodatkowo wskazanie osoby, osób lub organu do których wiadomości przekazano korespondencję, rodzaj listu (zwykły, polecony, email), oznaczenie czy korespondencja ma charakter przychodzący czy wychodzący, status korespondencji (załatwione albo niezałatwione), data wysłania.
4	**Dziennik Korespondencji Okręgowej Komisji Kwalifikacyjnej**	W zbiorze przetwarzane są dane osobowe: a) dla pism przychodzących: numer korespondencji na Dzienniku Korespondencji Okręgowej Komisji Kwalifikacyjnej, data wpływu pisma do Okręgowej Komisji Kwalifikacyjnej, numer pisma na Dzienniku Korespondencji Izby, data wpływu do Izby, nadawca (imię i nazwisko), treść korespondencji (tytuł lub skrótowo – ustalane indyw.), charakter sprawy (wybór jednego z listy – wniosek o nadanie uprawnień budowlanych, wniosek o nadanie uprawnień budowlanych wyznaczenie terminu, interpretacja uprawnień budowlanych, wniosek o zmianę decyzji, pismo w sprawie biegłego sądowego, wniosek o nadanie tytułu rzeczoznawcy budowlanego, wniosek o wydanie duplikatu decyzji, zapytanie dotyczące praktyki zawodowej, varia – inne pozostałe nieskalsyfikowane kategorie), numer postępowania, termin do załatwienia sprawy (niezwłocznie, 7 dni, miesiąc, dwa miesiące, pismo w sprawie), termin do załatwienia sprawy – data, uwagi, numer odpowiedzi na Dzienniku Korespondencji Okręgowej Komisji Kwalifikacyjnej; b) dla pism wychodzących: numer korespondencji na Dzienniku Korespondencji Okręgowej Komisji Kwalifikacyjnej, data sporządzenia pisma, numer pisma na Dzienniku Korespondencji Izby, data wysłania z Izby, adresat (imię i nazwisko), treść korespondencji (tytuł lub skrótowo – ustalane indyw.), numer pisma na które udzielana jest odpowiedź na Dzienniku Korespondencji Okręgowej Komisji Kwalifikacyjnej, numer

		poprzedniego pisma w sprawie na Dzienniku Korespondencji Okręgowej Komisji Kwalifikacyjnej, uwagi.
5	**Dziennik Korespondencji Okręgowego Sądu Dyscyplinarnego**	W zbiorze przetwarzane są dane osobowe: a) dla pism przychodzących: numer korespondencji na Dzienniku Korespondencji Okręgowego Sądu Dyscyplinarnego, data wpływu pisma do Okręgowego Sądu Dyscyplinarnego, numer pisma na Dzienniku Korespondencji Izby, data wpływu do Izby, nadawca (imię i nazwisko), treść korespondencji (tytuł lub skrótowo – ustalane indyw.), charakter sprawy (wybór jednego z listy – zawodowa, dyscyplinarna, sprawozdawczość/informacje dla organów nadrzędnych, organizacyjne, varia – inne pozostałe nieskalsyfikowane kategorie), termin do załatwienia sprawy (niezwłocznie, 7 dni, miesiąc, dwa miesiące, pismo w sprawie), termin do załatwienia sprawy – data, uwagi, numer odpowiedzi na Dzienniku Korespondencji Okręgowego Sądu Dyscyplinarnego, numer postępowania; b) dla pism wychodzących: numer korespondencji na Dzienniku Korespondencji Okręgowego Sądu Dyscyplinarnego, numer pisma na Dzienniku Korespondencji Izby, data wysłania z Izby, adresat (imię i nazwisko), treść korespondencji (tytuł lub skrótowo – ustalane indyw.), numer pisma na które udzielana jest odpowiedź na Dzienniku Korespondencji Okręgowego Sądu Dyscyplinarnego, numer poprzedniego pisma w sprawie na Dzienniku Korespondencji Okręgowego Sądu Dyscyplinarnego, uwagi, numer postępowania.
6	**Dziennik Korespondencji Okręgowego Rzecznika Odpowiedzialności Zawodowej**	W zbiorze przetwarzane są dane osobowe: a) dla pism przychodzących: numer korespondencji na Dzienniku Korespondencji Okręgowego Rzecznika Odpowiedzialności Zawodowej, data wpływu pisma do Okręgowego Rzecznika Odpowiedzialności Zawodowej, numer pisma na Dzienniku Korespondencji Izby, data wpływu do Izby, nadawca (imię i nazwisko), treść korespondencji (tytuł lub skrótowo – ustalane indyw.), charakter sprawy (wybór jednego z listy – zawodowa, dyscyplinarna, sprawozdawczość/informacje dla organów nadrzędnych, organizacyjne, varia – inne pozostałe nieskalsyfikowane kategorie), termin do załatwienia sprawy (niezwłocznie, 7 dni, miesiąc, dwa miesiące, pismo w sprawie), termin do załatwienia sprawy – data, uwagi, numer odpowiedzi na Dzienniku Korespondencji Okręgowego Rzecznika Odpowiedzialności Zawodowej, numer postępowania; b) dla pism wychodzących: numer korespondencji na Dzienniku Korespondencji Okręgowego Rzecznika Odpowiedzialności Zawodowej, numer pisma na Dzienniku Korespondencji Izby, data wysłania z Izby, adresat (imię i nazwisko), treść korespondencji (tytuł lub skrótowo – ustalane indyw.), numer pisma na które udzielana jest odpowiedź na Dzienniku Korespondencji Okręgowego Rzecznika Odpowiedzialności Zawodowej, numer poprzedniego pisma w sprawie na Dzienniku Korespondencji Okręgowego Rzecznika Odpowiedzialności Zawodowej, uwagi, numer postępowania.
7	**Rejestr egzaminacyjny**	W zbiorze przetwarzane są dane osobowe osób ubiegających się o nadanie uprawnień budowlanych: nazwisko, imię, numer Zespołu Egzaminacyjnego, informacja o poprawce ustnej (tak/nie), numer porządkowy z listy osób do egzaminu, informacja na temat poprawki (tak/nie), data złożenia wniosku o nadanie uprawnień budowlanych, data złożenia pierwszego wniosku o nadanie uprawnień budowlanych, numer ewidencyjny (bez łamania na rok), numer ewidencyjny pełny, informacja na temat płci (1-kobieta, 2 mężczyzna), drugie

		imię, kod pocztowy, poczta, adres (ulica, numer domu, numer mieszkania), miejscowość (w przypadku miasta Łodzi wskazanie dzielnicy), kwota wpłaty opłaty za postępowanie kwalifikacyjne, data wpłaty, informacja na temat poprawności wpłaty (tak/nie), informacja na temat braku wpłaty (tak/nie), numer specjalności (2 – konstrukcyjno-budowlana, 3 – inżynieryjna drogowa, 4 – inżynieryjna mostowa, 5 – inżynieryjna kolejowa w zakresie kolejowych obiektów budowlanych, 6 – inżynieryjna wyburzeniowa, 7 – instalacyjna w zakresie sieci, instalacji i urządzeń telekomunikacyjnych, 8 - instalacyjna w zakresie sieci, instalacji i urządzeń cieplnych, wentylacyjnych, gazowych, wodociągowych i kanalizacyjnych, 9 - instalacyjna w zakresie sieci, instalacji i urządzeń elektrycznych i elektroenergetycznych, 10 – inżynieryjna hydrotechniczna, 11 inżynieryjna kolejowa w zakresie sterowania ruchem kolejowym), zakres uprawnień (1 – projektowanie bez ograniczeń, 2 – kierowanie robotami budowlanymi bez ograniczeń, 3 – projektowanie i kierowanie robotami budowlanymi bez ograniczeń, 4 – projektowanie w ograniczonym zakresie, 5 – kierowanie robotami budowlanymi w ograniczonym zakresie, 6 – projektowanie i kierowanie robotami budowlanymi w ograniczonym zakresie), informacja dotycząca ograniczenia egzaminu z uwagi na wcześniej zdawany egzamin (tak/nie), wykształcenie – tytuł, kierunek wykształcenia, informacja dotycząca indywidulanego zakwalifikowania wykształcenia (tak/nie), data urodzenia, miejsce urodzenia, PESEL, numer telefonu stacjonarnego, numer telefonu komórkowego, email, adres do korespondencji (kod pocztowy, miejscowość, ulica, numer domu, numer mieszkania), adres stałego zamieszkania (kod pocztowy, miejscowość, ulica, numer domu, numer mieszkania), numer Zespołu Kwalifikacyjnego, informacja na temat uzupełniania (tak/nie), informacja na temat sporządzanie wezwań w toku postępowania kwalifikacyjnego (tak/nie), informacja na temat dopuszczenia do egzaminu (tak/nie), informacja na temat odmowy dopuszczenia do egzaminu (tak/nie), informacja na temat przyczyn odmowy, kwota wpłaty opłaty za postępowanie egzaminacyjne, data wpłaty, informacja na temat poprawności wpłaty (tak/nie), informacja na temat braku wpłaty (tak/nie), informacja o obecności na egzaminie (tak/nie), informacja o zdaniu egzaminu (tak/nie), informacja o niezdaniu egzaminu (tak/nie), informacja o zdaniu egzaminu pisemnego (tak/nie), informacja o niezdaniu egzaminu pisemnego (tak/nie), wynik egzaminu pisemnego, wynik egzaminu ustnego, informacja o niezdaniu egzaminu ustnego (tak/nie), imię i nazwisko odmienione (celownik, biernik, dopełniacz), numer egzaminu, grupa egzaminów, informacja na temat poprawki ustnej (tak/nie), sala egzaminu pisemnego, data poprzedniego egzaminu pisemnego dla poprawki ustnej.
8	**Rejestr spraw Okręgowego Sądu Dyscyplinarnego**	W zbiorze przetwarzane są dane osobowe: liczba porządkowa, data wpływu pisma do Okręgowego Sądu Dyscyplinarnego, numer pisma na Dzienniku Korespondencji Izby, wnioskodawca (wskazanie Rzecznika lub innej osoby - imię i nazwisko, w przypadku Rzecznika numer wniosku, data sporządzenia i skrótowo zarzuty), znak sprawy (sygnatura sprawy), tryb postępowania (zawodowy, dyscyplinarny, zatarcie kary), samodzielna funkcja techniczna osoby obwinionej (projektant, sprawdzający, osoba wykonująca nadzór autorski, kierownik budowy, kierownik robót, inspektor nadzoru inwestorskiego, osoba sprawująca kontrolę techniczną utrzymania obiektów budowlanych), terminy posiedzeń i innych czynności procesowych (data i czynność), rozstrzygnięcie Okręgowego Sądu Dyscyplinarnego (data, ukaranie, uniewinnienie, umorzenie, zatarcie kary), przekazanie do drugiej instancji (tak/nie), zakończenie postępowania (tak/nie), rozstrzygnięcie ostateczne (ukaranie, uniewinnienie,

		umorzenie, zatarcie kary), data uprawomocnienia decyzji, dane obwinionego (imię, nazwisko, adres zamieszkania - kod pocztowy, miejscowość, ulica, numer domu/mieszkania, miejsce czynu), skład orzekający (imiona i nazwiska sędziów), decyzja Okręgowego Sądu Dyscyplinarnego (numer i treść), drugi skład orzekający (imiona i nazwiska sędziów Krajowego Sądu Dyscyplinarnego), decyzja ostateczna (numer decyzji, data wydania decyzji, sentencja decyzji), status sprawy, inne uwagi.
9	**Rejestr spraw Okręgowego Rzecznika Odpowiedzialności Zawodowej**	W zbiorze przetwarzane są dane osobowe: liczba porządkowa, data wpływu pisma do Okręgowego Rzecznika Odpowiedzialności Zawodowej, data wpływu do Izby, numer pisma na Dzienniku Korespondencji Izby, znak sprawy (sygnatura sprawy i numer korespondencji na Dzienniku Korespondencji Okręgowego Rzecznika Odpowiedzialności Zawodowej), wnioskodawca/zawiadamiający (imię i nazwisko), obwiniony (imię, nazwisko, adres zamieszkania - kod pocztowy, miejscowość, ulica, numer domu/mieszkania, numer członkowski), inne dane obwinionego (wykształcenie obwinionego, numer uprawnień budowlanych, data wydania decyzji o nadaniu uprawnień budowlanych oraz specjalność), pokrzywdzony (imię, nazwisko, adres zamieszkania - kod pocztowy, miejscowość, ulica, numer domu/mieszkania, numer członkowski), Rzecznik prowadzący sprawę (imię, nazwisko, data wyznaczenia), przedmiot sprawy (charakter naruszonych przepisów lub obowiązków), tryb postępowania (zawodowy, dyscyplinarny, inne), data zakończenia postępowania, data rozstrzygnięć Okręgowego Rzecznika Odpowiedzialności Zawodowej (odmowy wszczęcia postępowania, umorzenia postępowania, zawieszenia postępowania, wznowienia postępowania po zawieszeniu, decyzji/postanowienia kończących sprawę), pisma do prokuratury, stanowisko prokuratury, przekazanie zgodnie z właściwością, wniosek do Okręgowego Sądu Dyscyplinarnego (numer wniosku, data złożenia), zwrot sprawy z Okręgowego Sądu Dyscyplinarnego – data, ponowne przekazanie do Okręgowego Sądu Dyscyplinarnego – data, odwołanie do Krajowego Rzecznika Odpowiedzialności Zawodowej (daty wysłania i zwrotu akt), orzeczenie Krajowego Rzecznika Odpowiedzialności Zawodowej (data wydania i treść – skrótowo), rozstrzygnięcie Okręgowego Sądu Dyscyplinarnego (data i treść skrótowo), stanowisko Okręgowego Rzecznika Odpowiedzialności Zawodowej do rozstrzygnięcia Okręgowego Sądu Dyscyplinarnego (uznanie albo odwołanie), uwagi.
10	**Rejestr kadrowo-płacowy**	W zbiorze przetwarzane są dane osobowe pracowników i kontrahentów Izby gromadzone dla celów rozliczeniowych: imię, nazwisko, PESEL, data urodzenia, płeć, imiona rodziców, adres zamieszkania (kod pocztowy, miejscowość, ulica, numer domu/mieszkania), adres zameldowania (kod pocztowy, miejscowość, ulica, numer domu/mieszkania), NIP, numer konta bankowego.

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI PROGRAMAMI.

Pomiędzy programami: Członkowie, Dziennik Korespondencji, Microsoft Excel, Microsoft Access oraz System enova365, używanymi w Izbie do przetwarzania danych osobowych w wyżej opisanych zbiorach danych nie występuje eksport danych.

Izba eksportuje i importuje dane osobowe w zbiorach danych Rejestr członków Izby i Rejestr potencjalnych członków Izby odpowiednio ze zbiorów danych osobowych Rejestr członków PIIB i Rejestr potencjalnych członków PIIB prowadzonych przez Krajową Radę Polskiej Izby Inżynierów Budownictwa w systemie informatycznym BUDINFO.

Rejestr członków Izby i Rejestr potencjalnych członków Izby eksportuje dane osobowe do Rejestr członków PIIB i Rejestr potencjalnych członków PIIB odpowiednio w zakresach: „Dane osobowe" – wszystkie pola informacyjne, „Adresy" – wszystkie pola informacyjne, „Dane członkowskie" – wszystkie pola informacyjne poza numerem konta bankowego do wpłaty składki członkowskiej na okręgową izbę oraz numerem konta bankowego do wpłaty składki członkowskiej na krajową izbę członkowski, „Finanse" – kwota i data wpłaty na konto bankowego do wpłaty składki członkowskiej na okręgową izbę, tytuł wpłaty oraz „Zawieszenia i skreślenia" – wszystkie pola informacyjne.

Rejestr członków Izby i Rejestr potencjalnych członków Izby importuje dane osobowe z Rejestru członków PIIB i Rejestru potencjalnych członków PIIB odpowiednio w zakresach:

a) „Dane członkowskie" – numer konta bankowego do wpłaty składki członkowskiej na okręgową izbę oraz numer konta bankowego do wpłaty składki członkowskiej na krajową izbę członkowski;
b) „Finanse" – kwota i data wpłaty na konto bankowego do wpłaty składki członkowskiej na krajową izbę, tytuł wpłaty;
c) „Zaświadczenia" – wszystkie pola informacyjne;
d) „Ubezpieczenia" – wszystkie pola informacyjne.

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE.

Polityka obowiązuje w Izbie, w pomieszczeniach lub częściach pomieszczeń, w których przetwarzane są dane osobowe, a których wykaz został zamieszczony poniżej.

Siedziba Izby mieści się pod adresem: ul. Północna 39, 90-425 Łódź.

1.	Wykaz pomieszczeń, w których przetwarzane są dane osobowe.	Pokoje nr: 01, 07 (archiwum), 1, 3 (serwerownia), 4, 5, 6 (sekretariat ogólny), 7, 8 (Dział Księgowy), 15 (Dział Prawny), 21, 22, 25 (Redakcja i Dział Szkoleń), 26.
2.	Wykaz pomieszczeń, w których znajdują się komputery stanowiące element systemu informatycznego	Pokoje nr: 1, 3 (serwerownia), 4, 5, 6 (sekretariat ogólny), 7, 8 (Dział Księgowy), 15 (Dział Prawny), 21, 22, 25 (Redakcja i Dział Szkoleń), 26.
3.	Wykaz pomieszczeń, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe)	Pokoje nr: a) 07 (archiwum) – dokumentacja papierowa obejmująca: korespondencję, akta postępowań prowadzonych przez organy Izby; b) 3 (serwerownia) – serwery podstawowy i z kopią zapasową danych. Na serwerach zapisane są wszystkie ww. zbiory danych osobowych; c) 6 (sekretariat ogólny) – dokumentacja papierowa obejmująca wnioski o wpisanie na listę członków Izby oraz bieżącą korespondencję; d) 15 (Dział Prawny) – dokumentacja papierowa obejmująca akta postępowań w toku prowadzonych przez Okręgową Komisję Kwalifikacyjną, Okręgowy Sąd

		Dyscyplinarny i Okręgowego Rzecznika Odpowiedzialności Zawodowej oraz bieżącą korespondencję wskazanych organów.
4.	Wykaz pomieszczeń, w których składowane są uszkodzone komputerowe nośniki danych w postaci dysków komputerowych, płyty CD oraz uszkodzonych komputerów i dysków.	Pokój nr 3 (Serwerownia).
5.	Wykaz pomieszczeń archiwum	Pokój nr 07.
6.	Wykaz programów, w których przetwarzane są dane osobowe	1) Członkowie; 2) Dziennik Korespondencji; 3) Microsoft Excel; 4) Microsoft Access; 5) System enova365.
7.	Wykaz podmiotów zewnętrznych, które mają dostęp do danych osobowych lub je przetwarzają.	Na chwilę przyjęcia instrukcji dostęp do danych osobowych w zakresie opisanym w Rozdziale: „Sposób przepływu danych pomiędzy poszczególnymi systemami" posiada wyłącznie Polska Izba Inżynierów Budownictwa.

ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH.

Środki techniczne:

1) Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony, przy czym budynek, w którym przetwarzane są dane osobowe podlega ochronie fizycznej w godz. 6 – 22 w dniach otwarcia Biura Izby oraz ochronie doraźnej w pozostałych godzinach i dniach, jak również stałemu monitoringowi zewnętrznych kamer przemysłowych.
2) Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych objęte są systemem kontroli dostępu.
3) Zbiory danych osobowych przechowywane są w pomieszczeniu serwerowni – pokój nr 3, zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
4) Zbiory danych osobowych lub wydruki danych z tych zbiorów w formie papierowej, o ile zostały sporządzone, przechowywane są w zamkniętych metalowych szafach.
5) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w pomieszczeniu serwerowni – pokój nr 3.
6) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego.
7) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
8) Nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.
9) Wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą - urządzenia stanowiącego bramę DNS oraz oprogramowania typu FireWall.
10) Stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową.
11) Komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła.
12) System informatyczny zabezpieczono za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła.

Środki organizacyjne:

1) Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.
2) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
3) Wyznaczono Administratora Systemu Informatycznego.
4) Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych.
5) Opracowano i wdrożono Instrukcję Zarządzania Systemem Informatycznym służącymi do przetwarzania danych osobowych.
6) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
7) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
8) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
9) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.

ZAŁĄCZNIKI.

Załącznik nr 1 – upoważnienie do przetwarzania danych osobowych.

Załącznik nr 2 – ewidencji upoważnień we wszystkich zbiorach danych osobowych

Załącznik nr 1

UPOWAŻANIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym jako Przewodnicząca Okręgowej Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa, reprezentując Administratora Danych – Łódzką Okręgową Izbę Inżynierów Budownictwa z siedzibą przy ul. Północnej 39, 90-425 w Łodzi, na mocy stosownego umocowania nadanego na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity Dz. U. z 2016 r., poz. 922*),

upoważniam do przetwarzania danych osobowych Pana/Panią:

……,

(zwaną dalej osobą upoważnioną).

Przedmiotowe upoważnienie obejmuje swoim zakresem następujące zbiory danych osobowych:

Nr	Nazwa zbioru danych osobowych
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem administratora danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity Dz. U. z 2016 r., poz. 922*), wydanych na jej podstawie aktów wykonawczych i obowiązujących w Łódzkiej Okręgowej Izbie Inżynierów Budownictwa wewnętrznych regulacji w sprawie ochrony danych osobowych.

Upoważnienie jest ważne do odwołania.

.....	.....
(Data i podpis osoby upoważnionej do przetwarzania danych osobowych)	(Data i podpis upoważniającego.)

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Łódzkiej Okręgowej Izbie Inżynierów Budownictwa, w szczególności z Polityką Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych. Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....

(Data i podpis pracownika)

Sporządzone 2 egz. w oryginale otrzymują:

1) Dział Księgowości Biura Łódzkiej Okręgowej Izby Inżynierów Budownictwa
2) pracownik uzyskujący upoważnienie.

Załącznik nr 2

EWIDENCJA UPOWAŻNIEŃ WE WSZYSTKICH ZBIORACH DANYCH OSOBOWYCH

Lp.	Nazwisko, Imię	Zbiory danych osobowych objęte upoważnieniem	Okres upoważnienia		Identyfikator dla poszczególnych Programów w Systemie Informatycznym	Uwagi
			od	do		
1						
2						
3						
4						
5						
...						

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

ŁÓDZKA OKRĘGOWA IZBA INŻYNIERÓW BUDOWNICTWA

www.lod.piib.org.pl

91-425 ŁÓDŹ

Ul. PÓŁNOCNA 39

NIP: 725-18-49-050

SPIS TREŚCI

INFORMACJE OGÓLNE.

Niniejszy dokument w postaci Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych został opracowany przez Administratora Danych – Łódzką Okręgową Izbę Inżynierów Budownictwa w celu zapewnienia zgodności przetwarzania danych osobowych z polskim prawem.

Instrukcja Zarządzania Systemem Informatycznym wraz z Polityką Bezpieczeństwa stanowi dokumentację przetwarzania danych osobowych w rozumieniu w rozumieniu art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity Dz. U. z 2016 r., poz. 922*) i § 1 pkt 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.*).

Instrukcja Zarządzania Systemem Informatycznym obowiązuje od dnia 1 października 2016 r. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Każda osoba mającą dostęp do danych osobowych na podstawie upoważnienia Administratora Danych, została zapoznana z Instrukcją Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych. Wyżej wymienione osoby złożyły na piśmie oświadczenie o zapoznaniu się z treścią Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych oraz zobowiązały się do stosowania zawartych w niej postanowień.

CEL PRZYGOTOWANIA INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH.

Podstawowym celem przyświecającym przygotowaniu i wdrożeniu dokumentu Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych, zwanej dalej Instrukcją, jest zapewnienie zgodności działania Izby i jej organów z ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi. Dokument Instrukcji został opracowany na podstawie przepisów zawartych w następujących aktach prawnych:

1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity Dz. U. z 2016 r., poz. 922*),
2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.*),
3) ustawa z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (*tekst jednolity Dz. U. z 2014 r., poz. 1946 z późn. zm.*),
4) Statut Polskiej Izby Inżynierów Budownictwa (w brzmieniu ustalonym *Uchwałą II. Nadzwyczajnego Krajowego Zjazdu Polskiej Izby Inżynierów Nr 8/15 z dnia 20 sierpnia 2015 r. zmieniająca uchwałę w sprawie uchwalenia statutu Polskiej Izby Inżynierów Budownictwa*),
5) Regulamin okręgowych rad Polskiej Izby Inżynierów Budownictwa (w brzmieniu ustalonym *Uchwałą II. Nadzwyczajnego Krajowego Zjazdu Polskiej Izby Inżynierów Nr 14/15 z dnia 20 sierpnia 2015 r. zmieniająca uchwałę w sprawie regulaminu okręgowych rad Polskiej Izby Inżynierów Budownictwa*).

Należy przez powyższe rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zadaniem Instrukcji Zarządzania jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i system informatyczny służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

ZAKRES INFORMACJI OBJĘTYCH INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH.

Dokument Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Obejmuje on ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, o zastosowanych rozwiązaniach technicznych, jak również o procedurach eksploatacji i zasady użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Na Instrukcję składają się w szczególności następujące informacje:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania:
   a) elektronicznych nośników informacji zawierających dane osobowe,
   b) kopii zapasowych, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia;
8) procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych.

Instrukcję Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych stosuje się do wszelkich czynności, stanowiących w myśl ustawy o ochronie danych osobowych przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosuje się zasady przetwarzania danych osobowych ujęte w niniejszym dokumencie Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych.

WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH.

1) **administrator danych** - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych, tj. Łódzką Okręgową Izbę Inżynierów Budownictwa, zwaną dalej „Izbą",
2) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3) **hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
4) **identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
5) **instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych** - dokument instrukcji zarządzania systemem informatycznym w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „Instrukcją",
6) **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
7) **odbiorca danych** - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby upoważnionej do przetwarzania danych,
    c) przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
    d) podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
    e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
8) **państwo trzecie** - rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego,
9) **Polityka Bezpieczeństwa** – dokument Polityki Bezpieczeństwa w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „Polityką",

10) **poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
11) **przetwarzanie danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym,
12) **raport** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
13) **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
14) **rozporządzenie** – rozumie się przez to rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.*), zwane dalej „rozporządzeniem",
15) **sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (*Dz. U. z 2000 r., Nr 73, poz. 852 z późn. zm.*) i publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne (*tekst jednolity Dz. U. z 2014 r., poz. 243 z późn. zm.*),
16) **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (*Dz. U. z 2000 r., Nr 73, poz. 852 z późn. zm.*) i sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne (*tekst jednolity Dz. U. z 2014 r., poz. 243 z późn. zm.*),
17) **system informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
18) **teletransmisja** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
19) **ustawa** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity Dz. U. z 2016 r., poz. 922*), zwaną dalej „ustawą",

20) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
21) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
22) **zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
23) **zbiór danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
24) **zgoda osoby, której dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSÓB ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

1. Uprawnienia do przetwarzania danych osobowych w systemie informatycznym nadaje każdorazowo Administrator Systemu Informatycznego.
2. W celu nadania uprawnienia o którym mowa w pkt 1, lub zmiany jego zakresu Dyrektor Biura Łódzkiej Okręgowej Izby Inżynierów Budownictwa lub zainteresowany pracownik występuje z umotywowanym wnioskiem do Administratora Systemu Informatycznego.
3. Uprawnienie do przetwarzania danych osobowych w systemie informatycznym może zostać nadane wyłącznie pracownikom, którzy uzyskali upoważnienie do przetwarzania danych osobowych nadane przez Przewodniczącą Okręgowej Rady.
4. Administrator Systemu Informatycznego każdorazowo decyduje czy istnieje konieczność (w celu wykonywania obowiązków zawodowych) nadania upoważnionemu pracownikowi uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
5. Zakres uprawnienia (zakres dostępu do danych osobowych przetwarzanych w systemie informatycznym) nie może być szerszy niż w wydanym wcześniej upoważnieniu.
6. Przydzielanie poszczególnym pracownikom uprawnień do przetwarzania danych osobowych w systemie informatycznym następuje poprzez nadanie im loginu oraz hasła tymczasowego pozwalającego na dostęp do danego systemu informatycznego (zgodnie z trybem określonym w Rozdziale „Opis stosowanych metod i środków uwierzytelnienia oraz procedur związanych z zarządzaniem i użytkowaniem stosowanych metod i środków uwierzytelnienia" niniejszej Instrukcji).
7. Administrator Systemu Informatycznego prowadzi rejestr nadanych uprawnień do przetwarzania danych w systemie informatycznym.
8. Jeśli Administrator Systemu Informatycznego uzna to za stosowne, uprawnienie dostępu do danego systemu informatycznego może zostać w każdej chwili cofnięte poprzez ograniczenie/ uniemożliwienie dostępu do przetwarzania danych w systemie informatycznym.
9. Cofnięcie uprawnienia dostępu do systemu informatycznego Administrator Systemu Informatycznego odnotowuje w prowadzonym przez siebie w rejestrze nadanych uprawnień.
10. Administrator Systemu Informatycznego jest odpowiedzialny za:
    a) przegląd przestrzegania Instrukcji;

b) przegląd aktualności Instrukcji;

c) nadawanie uprawnień do przetwarzania danych w systemie informatycznym;

d) rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym;

e) wyrejestrowanie uprawnień do przetwarzania danych w systemie informatycznym.

OPIS STOSOWANYCH METOD I ŚRODKÓW UWIERZYTELNIENIA ORAZ PROCEDUR ZWIĄZANYCH Z ZARZĄDZANIEM I UŻYTKOWANIEM STOSOWANYCH METOD I ŚRODKÓW UWIERZYTELNIENIA.

1. Dla każdego użytkownika systemu informatycznego ustala się odrębne konto zawierające w szczególności: identyfikator, hasło pierwszego logowania, dane o uprawnieniach użytkownika, profil.
2. Hasła tymczasowe do konta użytkownika (w przypadku utworzenia nowego konta, a także w sytuacjach awaryjnych związanych np.: z zagubieniem, utratą lub zapomnieniem hasła osobistego przez użytkownika konta) tworzone są przez Administratora Systemu Informatycznego.
3. Tryb przekazywania ww. hasła tymczasowego odbywa się w sposób zapewniający bezpieczeństwo i poufność przekazywanych informacji, w szczególności: w sposób uniemożliwiający innej osobie ich podsłuchanie lub nieuprawnione wykorzystanie.
4. Zezwala się na wykorzystanie innych, niewymienionych w Rozdziale 3 pkt. 3 niniejszej Instrukcji, bezpiecznych metod i środków technicznych, w celu przekazania hasła tymczasowego, za pisemną zgodą Administratora Systemu Informatycznego.
5. Zakazuje się przekazywania haseł tymczasowych poprzez osoby trzecie lub przy użyciu metod, które nie gwarantują zachowania jego poufności oraz niezaprzeczalnego ustalenia nadawcy i odbiorcy hasła, np.: przez niechronione wiadomości przekazywane elektronicznie.
6. Po otrzymaniu hasła tymczasowego użytkownik ma obowiązek niezwłocznego zalogowania się do systemu informatycznego przy użyciu tego hasła oraz jego zmiany na hasło osobiste.
7. Ujawnianie przez użytkownika komukolwiek, jakichkolwiek aktualnych lub poprzednich haseł tymczasowych, haseł osobistych lub innych haseł mu powierzonych, jest zabronione.
8. Autoryzacja do wszystkich programów przetwarzających dane osobowe, opisanych w niniejszej Instrukcji możliwa jest wyłącznie za pomocą loginu i hasła.
9. Jeżeli do uwierzytelniania użytkowników używa się hasła, jego zmiana musi następować nie rzadziej niż co 30 dni, hasło musi się składać z co najmniej 8 znaków długości oraz jednocześnie zawierać małe i wielkie litery, cyfry lub znaki specjalne.
10. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa haseł i innych identyfikatorów pozwalających na autoryzację w programach przetwarzających dane

osobowe nie zaleca się stosowania jakichkolwiek programów i systemów umożliwiających zapamiętywanie identyfikatorów i haseł. Nie ma możliwości zapamiętania hasła użytkownika do systemu operacyjnego.

11. Dostęp do każdego z profili użytkowników ograniczony jest wyłącznie do jednego pracownika.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU.

Procedura rozpoczęcia pracy.

Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy, każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły objawy, mogące świadczyć o naruszeniu zasad ochrony danych osobowych.

Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu. Użytkownikowi nie wolno w czasie uruchamiania systemu operacyjnego odchodzić od stanowiska. Jest to dozwolone tylko i wyłącznie zgodnie z procedurą opisującą tryb zawieszenia pracy z systemem, w którym przetwarzane są dane osobowe.

Użytkownik informuje Administratora Systemu Informatycznego lub osobę przez niego upoważnioną do opieki nad sprzętem komputerowym o wszelkich nieprawidłowościach w dostępie do systemu informatycznego.

Procedura zawieszenia pracy.

1) W przypadku konieczności zawieszenia pracy w systemie informatycznym z powodu tymczasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest, w zależności od przewidywanego okresu swojej nieobecności, do aktywowania wygaszacza ekranu, zabezpieczonego hasłem lub do zablokowania dostępu do użytkowanego systemu komputerowego poprzez jednoczesne naciśnięcie klawiszy {Ctrl + Alt + Delete} i potwierdzenia klawiszem Enter podświetlonej opcji „Zablokuj komputer".
2) Krótkotrwałe przerwy w pracy bez opuszczania stanowiska pracy nie wymagają zamykania aplikacji i wylogowania się z systemu.

Procedura zakończenia pracy.

Zakończenie pracy polega na wybraniu odpowiedniego polecenia systemowego umożliwiającego zakończenie pracy. Zaleca się zamknięcie wszystkich programów i zapisanie wszystkich otwartych plików. Użytkownik powinien pozostać przy komputerze do chwili jego wyłączenia.

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA.

1. Administrator Systemów Informatycznych sprawuje ogólny nadzór nad prawidłowym przebiegiem procedury sporządzania kopii zapasowych przetwarzanych zbiorów danych osobowych oraz kopii programów informatycznych używanych do ich przetwarzania.
2. Wszystkie programy służące do przetwarzania danych osobowych wymienione w Polityce są zapisane na serwerze Izby znajdującym się w pomieszczeniu serwerowni (pokój nr 3).
3. Kopie zapasowe tworzone są codziennie w sposób automatyczny dane zapisywane są na dwa oddzielne dyski serwera Izby.
4. Niezależnie od wykonywanych kopii zapasowych tworzonych w sposób automatyczny dwa razy w miesiącu dokonuje się zapisu danych na nośnikach zewnętrznych.
5. Nośniki zawierające kopie zapasowe baz z danymi osobowymi po ustaniu ich użyteczności podlegają likwidacji poprzez pozbawienie ich zapisu tych danych, a gdy nie jest to możliwe, nośniki danych uszkadza się fizycznie w sposób uniemożliwiający odczytanie zapisanych danych poprzez rozdrobnienie lub spalenie. Z tych czynności Administrator Systemu Informatycznego sporządza protokół.
6. Przebywanie osób nieuprawnionych do przetwarzania danych osobowych w pomieszczeniu serwerowni (pokój nr 3) dopuszczalne jest za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
7. Na wniosek Administratora Systemu Informatycznego inicjowane są działania mające na celu wzmocnienie bezpieczeństwa przy przetwarzaniu danych osobowych w systemach informatycznych, oraz informowanie Dyrektora Biura Izby o konieczności wprowadzenia zmian w istniejących procedurach.

OPIS SPOSOBU, MIEJSCA I OKRESU PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH.

1) Kopie zapasowe przechowywane są w siedzibie Izby w pokój nr 5 oraz na serwerze znajdującym się w pomieszczeniu serwerowni (pokój nr 3) w siedzibie Izby. Dostęp do wskazanych pomieszczeń mają wyłącznie Dyrektor Biura Izby, Administrator Systemu Informatycznego oraz upoważnieni pracownicy Izby.
2) Kopie zapasowe przechowywane są przez 1 rok, chyba że zewnętrzne przepisy wymagają dłuższego okresu przechowywania.

OPIS SPOSOBU ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, O KTÓRYM MOWA W PKT III PPKT 1 ZAŁĄCZNIKA DO ROZPORZĄDZENIA.

Z uwagi na fakt, iż komputery przetwarzające dane osobowe posiadają dostęp do sieci publicznej, Administrator Danych wdrożył procedury oraz oprogramowanie, które chroni dane osobowe przed nieuprawnionym dostępem, zmianom, usunięciem lub uszkodzeniem. Zagrożenia te to programy zawierające złośliwy kod (wirusy), tzw. konie trojańskie oraz ataki hakerów.

Aby zmniejszyć to zagrożenie, zabronione jest pobieranie oraz instalowanie na komputerach, bez nadzoru Administratora Systemu Informatycznego, jakichkolwiek programów służących do przetwarzania danych osobowych.

Zabronione jest również używanie nośników informacji niepochodzących z zasobów Administratora Danych. Każda osoba przetwarzająca dane osobowe przy użyciu komputera została pouczona, aby w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych, poinformowała o tym fakcie osobę upoważnioną przez Administratora Danych lub Administratora Systemu Informatycznego.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej stosowane do zabezpieczenia systemu informatycznego:

1) Zastosowano urządzenia typu UPS, chroniące system informatyczny (serwer i poszczególne komputery stacjonarne), służący do przetwarzania danych osobowych przed skutkami awarii zasilania
2) Dostęp do systemu informatycznego (lokalna sieć Izby) został zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. W ten sam sposób zabezpieczono wszystkie komputery przed nieautoryzowanym uruchomieniem.
3) Administrator systemu informatycznego na zlecenie Dyrektora Biura określa zakres obszarów systemu dostępnych dla poszczególnych użytkowników sieci lokalnej Izby.
4) Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
5) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
6) Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
7) Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.

8) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
9) Użyto system Firewall do ochrony dostępu do sieci komputerowej.
10) W ramach narzędzi programowych i baz danych zastosowano następujące środki ochrony:

a) Każdy programów przetwarzających dane osobowe został zabezpieczonym oddzielnym hasłem.
b) Administrator systemu informatycznego na zlecenie Dyrektora Biura określa zakresy poszczególnych programów dostępne dla uprawnionych programu użytkowników.
c) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
d) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

OPIS SPOSOBU REALIZACJI WYMOGÓW STAWIANYCH SYSTEMOWI INFORMATYCZNEMU PRZEZ ROZPORZĄDZENIE WYKONAWCZE DO USTAWY O OCHRONIE DANYCH OSOBOWYCH.

Nazwa programu **Wymogi rozporządzenia**	**Członkowie ŁOIIB**	**Dziennik Korespondencji**	**Microsoft Excel**	**Microsoft Access**	**System enova365**
Progami rejestruje datę wprowadzenia danych do programu.	TAK	TAK	TAK	TAK	TAK
Program rejestruje identyfikator użytkownika wprowadzającego dane osobowe do programu, chyba że dostęp do programu i przetwarzanych w nim danych posiada wyłącznie jedna osoba.	TAK	TAK	Do poszczególnych zbiorów danych osobowych posiadają wyłącznie pojedynczy użytkownicy.		TAK
Program rejestruje źródło danych, w przypadku zbierania danych, nie od osoby, której one dotyczą.	Dane osobowe przetwarzane w programach pochodzą od osób, których dane dotyczą.				
Program rejestruje informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że program używany jest do przetwarzania danych zawartych w zbiorach jawnych.	Dla każdego programu prowadzona oddzielna lista dotycząca udostępnień.				
Program rejestruje sprzeciw o którym mowa w art. 32 ust. 1 pkt. 8 ustawy.	TAK	Dla każdego programu prowadzona oddzielna lista sprzeciwów.			

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH.

1. O przeprowadzanych przeglądach i konserwacjach systemu informatycznego informowany jest Dyrektor Biura Izby i Administrator Systemu Informatycznego (o ile sam bezpośrednio nie przeprowadza tych czynności), którzy mogą uczestniczyć w dokonywanych czynnościach.
2. Wstępne przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych a także wstępne czynności serwisowe dokonywane są w siedzibie Izby.
3. W wypadku wystąpienia takiej potrzeby przegląd i konserwacja mogą być zlecone pracownikowi lub podmiotowi zewnętrznemu specjalizującemu się w tego typu działaniach.
4. W wypadku przekazania sprzętu lub nośników informacji służących do przetwarzania danych osobowych podmiotowi trzeciemu, pozbawia się je zapisanych danych osobowych w sposób, który uniemożliwi ich odtworzenie. W obydwu przypadkach, zostaną zachowane szczególne warunki ostrożności, w celu zabezpieczenia danych osobowych przed dostępem osób nieuprawnionych.
5. Jeśli Administrator Systemu Informatycznego nie dokonuje naprawy osobiście, podmiot dokonujący wyeliminowania opisanych nieprawidłowości, zawiadamia o podjętych czynnościach Administratora Systemu Informatycznego.
6. Wykryte podczas przeglądu i konserwacji nieprawidłowości w działaniu sprzętu lub programów służących do przetwarzania danych osobowych, usuwa się niezwłocznie.
7. Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu informatycznego odpowiada Administrator Systemu Informatycznego.

POZIOM BEZPIECZEŃSTWA.

Administrator Danych zastosował środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczył dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Administrator Danych zastosował dla wszystkich zbiorów danych i programów stosowanych do przetwarzania zbiorów danych osobowych środki bezpieczeństwa na poziomie wysoki, z uwagi iż urządzenia systemu informatycznego, służącego do przetwarzania danych osobowych, połączone są z siecią publiczną.

Zastosowano następujące zabezpieczenia:

1) Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
2) Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
3) Stosowane są mechanizmy kontroli dostępu do danych.
4) Jeżeli dostęp do danych posiadają co najmniej dwie osoby to w systemie rejestrowany jest dla każdego użytkownika odrębny identyfikator oraz dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
5) System jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.
6) System jest zabezpieczony przed utratą danych spowodowaną utratą zasilania lub zakłóceniami w sieci zasilającej.
7) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.
8) W przypadku gdy do uwierzytelnienia użytkowników używa się haseł, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne jego zmiana następuje nie rzadziej niż co 30 dni.

9) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych osobowych.
10) Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności.
11) Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
12) Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.
13) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
    a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
    c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
14) Urządzenia i nośniki zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych
15) Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.
16) System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

Uchwała Nr 7/PR/16

Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa

z dnia 28 lipca 2016 r.

w sprawie przyznania odznak honorowych

Polskiej Izby Inżynierów Budownictwa.

§ 1

Na podstawie art. 19 ust. 1 pkt 1 ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (tekst jedn. Dz.U. z 2014 r., poz. 1946), § 5 ust. 1 pkt 5 i 6 Regulaminu okręgowych rad Polskiej Izby Inżynierów Budownictwa uchwalonego w dniu 27 września 2002 r. przez I Krajowy Zjazd Polskiej Izby Inżynierów Budownictwa (*ost. popr. i uzup. Uchwałą II Nadzwyczajnego Krajowego Zjazd PIIB nr 14/15 z dnia 20 sierpnia 2015 r.*) oraz zgodnie z zgodnie z § 4 ust. 2 pkt 3 Regulaminu nadawania Odznaki Honorowej Polskiej Izby Inżynierów Budownictwa przyjętego w dniu 17 czerwca 2011 r. przez X Krajowy Zjazd Polskiej Izby Inżynierów Budownictwa uchwałą Nr 22/11, Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa rekomenduje Krajowej Radzie Polskiej Izby Inżynierów Budownictwa do odznaczenia Złotą Odznaką Honorową Polskiej Izby Inżynierów Budownictwa koleżankę dr hab. inż. Budownictwa Renatę Kotynię (nr ewid. ŁOD/BO/1829/02).

§ 2

Wymagana przepisem § 5 ust. 2 Regulaminu nadawania Odznaki Honorowej Polskiej Izby Inżynierów Budownictwa, stanowiącego załącznik do Uchwały nr 22/11 uchwalonej w dniu 17 czerwca 2011 r. przez X Krajowy Zjazd PIIB, informacja dotycząca kandydata, stanowi załączniki do niniejszej uchwały.

§ 3

Uchwała wchodzi w życie w dniu podjęcia.

Sekretarz Rady ŁOIIB

mgr inż. Grzegorz Rakowski

Przewodnicząca Rady ŁOIIB

mgr inż. Barbara Malec

ŁÓDZKA
OKRĘGOWA
IZBA
INŻYNIERÓW
BUDOWNICTWA

91-425 Łódź, ul. Północna 39
Tel./fax: 42 632 97 39, 42 630 56 39
e-mail: lod@piib.org.pl
www.lod.piib.org.pl
NIP: 725-18-49-050

Łódź, dnia 28 lipca 2016 r.

Łódzka Okręgowa Izba
Inżynierów Budownictwa
91-425 Łódź,ul. Północna 39
tel./fax 42 632 97 39, 42 630 56 39
www.lod.piib.org.pl
lod@piib.org.pl

Krajowa Rada
Polskiej Izby Inżynierów Budownictwa

Wniosek
o nadanie Złotej Odznaki Honorowej
Polskiej Izby Inżynierów Budownictwa

Imię i nazwisko: Renata Kotynia

Numer Członkowski: ŁOD/BO/1892/02

Tytuł zawodowy: dr hab. inż. budownictwa, prof. Politechniki Łódzkiej

Uzasadnienie wniosku: Członek Łódzkiej Okręgowej Izby Inżynierów Budownictwa od 1 stycznia 2003 r. W dniu 24 kwietnia 2013 r. otrzymała Srebrną odznakę honorową PIIB.

Aktywnie uczestniczy w przygotowaniu konferencji naukowych organizowanych przez ŁOIIB, w szczególności jej praca była nieoceniona podczas konferencji „Nowoczesne technologie – wybrane zagadnienia" (03.2016). Służy wiedzą i doświadczeniem Okręgowej Radzie w sprawach z zakresu promowania nowych technologii. Jest stałym autorem artykułów w „Kwartalniku Łódzkim" o tematyce związanej z budownictwem (ostatnio: „Pionierskie wzmocnienia kablobetonowych dźwigarów" KŁ nr I/2015 „Seminarium Cost Action TU1207" KŁ nr II/2016) Dzięki jej ofiarności i pracy Izba podtrzymuje ścisłe więzy z Wydziałem Budownictwa, Architektury i Inżynierii Środowiska Politechniki Łódzkiej, w tym z młodymi inżynierami.

Uchwała Nr 8/PR/16

Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa

z dnia 8 września 2016 r.

w sprawie przyznania zapomóg.

§ 1

Zgodnie z § 10 Zasad Gospodarki Finansowej Polskiej Izby Inżynierów Budownictwa, przyjętych uchwałą VII Krajowego Zjazdu Polskiej Izby Inżynierów Budownictwa Nr 28/08 z dnia 21 czerwca 2008 r. „Zasad gospodarki finansowej Polskiej Izby Inżynierów Budownictwa" (*ost. popr. i uzup. Uchwałą XIV Krajowego Zjazdu PIIB nr 18/15 z dnia 20 czerwca 2015 r.*) oraz na podstawie § 2 ust. 2 i § 4 ust. 2 Regulaminu działalności samopomocowej Łódzkiej Okręgowej Izby Inżynierów Budownictwa, przyjętego uchwałą Okręgowej Rady ŁOIIB Nr 26/R/14 z dnia 11 grudnia 2014r., Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa na wniosek Zespołu Rady ds. Działalności Samopomocowej postanawia udzielić:

1) Grażynie Cieślak w związku ze śmiercią męża Ryszarda Cieślaka, nr członkowski ŁOD/BO/7296/06 (wniosek 69/IV/16), jednorazowej zapomogi pośmiertnej w wysokości 2000,00 zł;
2) Elżbiecie Mateusiak w związku ze śmiercią męża Zbigniewa Mateusiaka, nr członkowski ŁOD/BO/5874/04 (wniosek 70/IV/16), jednorazowej zapomogi pośmiertnej w wysokości 2000,00 zł;
3) Stanisławie Strumińskiej w związku ze śmiercią męża Józefa Strumińskiego, nr członkowski ŁOD/BO/1711/02 (wniosek 71/IV/16), jednorazowej zapomogi pośmiertnej w wysokości 2000,00 zł;
4) Wojciechowi Kurkowskiemu w związku ze śmiercią ojca Ireneusza Kurkowskiego, nr członkowski ŁOD/BO/6331/04 (wniosek 72/IV/16), jednorazowej zapomogi pośmiertnej w wysokości 2000,00 zł;
5) Ewie Ozimek w związku ze śmiercią ojca Kazimierza Domagały, nr członkowski ŁOD/BO/3544/03 (wniosek 73/IV/16), jednorazowej zapomogi pośmiertnej w wysokości 2000,00 zł;
6) Annie Wawrzonek w związku ze śmiercią ojca Zbigniewa Cichońskiego, nr członkowski ŁOD/IS/2504/02 (wniosek 77/IV/16), jednorazowej zapomogi pośmiertnej w wysokości 2000,00 zł;
7) Wiesławie Siekierze w związku ze śmiercią męża Stanisława Siekiery, nr członkowski ŁOD/IE/3320/03 (wniosek 78/IV/16), jednorazowej

zapomogi pośmiertnej w wysokości 2000,00 zł.

§ 2

Zgodnie z § 10 Zasad Gospodarki Finansowej Polskiej Izby Inżynierów Budownictwa, przyjętych uchwałą VII Krajowego Zjazdu Polskiej Izby Inżynierów Budownictwa Nr 28/08 z dnia 21 czerwca 2008 r. „Zasad gospodarki finansowej Polskiej Izby Inżynierów Budownictwa" (*ost. popr. i uzup. Uchwałą XIV Krajowego Zjazdu PIIB nr 18/15 z dnia 20 czerwca 2015 r.*) oraz na podstawie § 2 ust. 2 i § 4 ust. 1 Regulaminu działalności samopomocowej Łódzkiej Okręgowej Izby Inżynierów Budownictwa, przyjętego uchwałą Okręgowej Rady ŁOIIB Nr 26/R/14 z dnia 11 grudnia 2014r., Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa na wniosek Zespołu Rady ds. Działalności Samopomocowej postanawia udzielić:

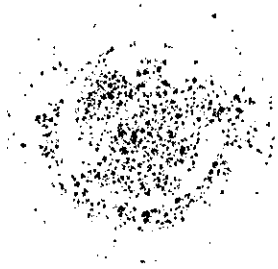
1) Zygmuntowi Karkowskiemu nr członkowski ŁOD/BO/5547/03 (wniosek 74/IV/16), w związku z długotrwałą chorobą - jednorazowej zapomogi w wysokości 3500,00 zł;
2) Krzysztofowi Denuszkowi nr członkowski ŁOD/BO/6541/04 (wniosek 75/IV/16), w związku z długotrwałą chorobą - jednorazowej zapomogi w wysokości 3500,00 zł;
3) Beacie Ciborskiej nr członkowski ŁOD/BO/0982/02 (wniosek 76/IV/16), w związku z długotrwałą chorobą - jednorazowej zapomogi w wysokości 3500,00 zł.

§ 3

Uchwała wchodzi w życie w dniu podjęcia.

Sekretarza Rady ŁOIIB — Przewodnicząca Rady ŁOIIB

mgr inż. Grzegorz Rakowski — mgr inż. Barbara Malec



Uchwała Nr 9/PR/16

Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa

z dnia 8 września 2016 r.

w sprawie przyznania dofinansowania.

Na podstawie art. 19 ust. 1 pkt 1 ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (*tekst jednolity Dz.U. z 2014 r., poz. 1946 z późn. zm.*), oraz zgodnie z § 4 Regulaminu dofinansowania doskonalenia zawodowego dla członków Łódzkiej Okręgowej Izby Inżynierów Budownictwa przyjętego Uchwałą Rady Nr 30/R/15 z dnia 10 grudnia 2015 r., Prezydium Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa na wniosek Zespołu ds. Doskonalenia Zawodowego przyznaje następującym osobom dofinansowanie:

1) Kazimierzowi Knapkiewiczowi nr członkowski ŁOD/IS/3777/03 dofinansowanie udziału w kursie językowym z technicznymi elementami języka branżowego związanym bezpośrednio z budownictwem w wysokości 446,50 zł;
2) Katarzynie Krzak nr członkowski ŁOD/IS/5072/03 dofinansowanie zakupu programu komputerowego związanego bezpośrednio z budownictwem i wykonywaniem zawodu inżyniera budownictwa w łącznej wysokości 737,50 zł;
3) Michałowi Bortkiewiczowi nr członkowski ŁOD/BO/8932/10 dofinansowanie zakupu programu komputerowego związanego bezpośrednio z budownictwem i wykonywaniem zawodu inżyniera budownictwa w łącznej wysokości 1000,00 zł;
4) Hubertowi Kotyni nr członkowski ŁOD/BO/0013/15 dofinansowanie zakupu programu komputerowego związanego bezpośrednio z budownictwem i wykonywaniem zawodu inżyniera budownictwa w łącznej wysokości 900,00 zł;

5) Marcinowi Kaźmierczakowi nr członkowski ŁOD/IS/8934/10 dofinansowanie udziału w szkoleniu związanym bezpośrednio z budownictwem w wysokości 525,00 zł;
6) Czesławowi Regule nr członkowski ŁOD/BO/7130/05 dofinansowanie udziału w kursie językowym z technicznymi elementami języka branżowego związanym bezpośrednio z budownictwem w wysokości 394,00 zł;
7) Piotrowi Parkitnemu nr członkowski ŁOD/BO/1150/02 dofinansowanie zakupu programu komputerowego związanego bezpośrednio z budownictwem i wykonywaniem zawodu inżyniera budownictwa w łącznej wysokości 1000,00 zł;
8) Jolancie Balcer nr członkowski ŁOD/BD/2122/02 dofinansowanie udziału w szkoleniu i konferencji związanych bezpośrednio z budownictwem w wysokości 300,00 zł;
9) Karolowi Matoszkowi nr członkowski ŁOD/IS/9276/11 dofinansowanie udziału w szkoleniu związanym bezpośrednio z budownictwem w wysokości 645,75 zł;
10) Joannie Owczarek nr członkowski ŁOD/BO/7911/07 dofinansowanie udziału w kursie językowym z technicznymi elementami języka branżowego związanym bezpośrednio z budownictwem w wysokości 394,00 zł;
11) Bożenie Wojtaszek nr członkowski ŁOD/BO/9385/11 dofinansowanie udziału w szkoleniu związanym bezpośrednio z budownictwem w wysokości 645,75 zł;
12) Piotrowi Kozłowskiemu nr członkowski ŁOD/IS/9092/10 dofinansowanie udziału w kursie językowym z technicznymi elementami języka branżowego związanym bezpośrednio z budownictwem w wysokości 690,00 zł;
13) Michałowi Stadnikowi nr członkowski ŁOD/BO/9386/11 dofinansowanie udziału w szkoleniu związanym bezpośrednio z budownictwem w wysokości 645,75 zł;
14) Przemysławowi Lisowskiemu nr członkowski ŁOD/BD/0223/14

dofinansowanie udziału w kursie językowym z technicznymi elementami języka branżowego związanym bezpośrednio z budownictwem w wysokości 375,00 zł.

§ 2

Uchwała wchodzi w życie w dniu podjęcia.

Sekretarza Rady ŁOIIB
mgr inż. Grzegorz Rakowski

Przewodnicząca Rady ŁOIIB
mgr inż. Barbara Malec