POLITYKA OCHRONY DANYCH OSOBOWYCH

Metal-Fach Jacek Kucharewicz

Na podstawie art. 24 Rozporządzenia 2016/679, z dniem 1.09.2018 r. wprowadza się Politykę ochrony danych osobowych

Sprawdził:		**Data:**	
Zatwierdził:		**Data:**	
Obowiązuje do:			
Wymagania prawne:	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 018 r., poz. 1000).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).		

METAL-FACH
Jacek Kucharewicz
ul. Sikorskiego 66, 16-100 Sokółka
tel. 85 711 94 54, fax. 85 711 94 54 wew. 30
NIP: 545-100-10-62, REGON: 050073833
e-mail: sprzedaz@metalfach.com.pl
www.metalfachtg.com.pl

SPIS TREŚCI:

1. Wykaz podstawowych skrótów

Skrót	Opis
u.o.d.o.	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. poz. 1000)
RODO	Rozporządzenie Parlamentu Europejskiego o Rady EU 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych)
rozp. MSWIA	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
UODO	Urząd Ochrony Danych Osobowych
ADO	Administrator Danych Osobowych
IOD	Inspektor Ochrony Danych
ASI	Administrator Systemów Informatycznych
SI	System Informatyczny
SZBDO	System Zarządzania Bezpieczeństwem Danych Osobowych
PODO	Polityka Ochrony Danych Osobowych
IZSI	Instrukcja Zarządzania Systemami Informatycznymi

2. Wykaz podstawowych definicji

Ilekroć w niniejszej Polityce Bezpieczeństwa mowa o:

1. **Administratorze Danych Osobowych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych;
2. **Inspektor Ochrony Danych** – rozumie się przez to osobę fizyczną wyznaczoną przez Administratora Danych Osobowych, o którym mowa w art. 8 u.o.d.o.;
3. **Administratorze Systemów Informatycznych** – rozumie się przez to wyznaczoną przez Administratora Danych Osobowych osobę lub podmiot zewnętrzny, odpowiedzialny za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;
4. **Osobie upoważnionej** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Użytkownikiem może być pracownik firmy, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż.
5. **Danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;
6. **Zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
7. **Przetwarzaniu danych osobowych** – 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 systemach informatycznych;
8. **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
9. **Zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przed ich nieuprawnionym przetwarzaniem;
10. **Bezpieczeństwie informacji** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania informacji by w każdych okolicznościach dostęp do nich był zgodny z założeniami;

11. **Usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

12. **Zgodzie 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;

13. **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe za wyjątkiem:

- osoby, której dane dotyczą,
- osoby upoważnionej do przetwarzania danych osobowych,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

14. **Państwie trzecim** – rozumie się przez to państwo należące do Europejskiego Obszaru Gospodarczego;

15. **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi uprawnionemu do pracy w systemie informatycznym;

16. **Identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w wyznaczonych obszarach systemu informatycznego firmy;

17. **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

18. **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

19. **Rozliczalności danych** – rozumie się przez to właściwość zapewniającą, że działania osoby lub podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie lub podmiotowi;

20. **Użytkowniku systemu informatycznego** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w systemach informatycznych, której nadano unikalny identyfikator i hasło;

21. **Uwierzytelnieniu** – rozumie się przez to proces poprawnej identyfikacji użytkownika systemu informatycznego w stopniu umożliwiającym przyznanie odpowiednich uprawnień lub przywilejów w systemie informatycznym firmy;

22. **Incydencie** – rozumie się przez to naruszenie bezpieczeństwa danych osobowych ze względu na poufność, dostępność i integralność;

23. **Zagrożeniu** - rozumie się przez to potencjalną możliwość wystąpienia incydentu;

24. **Działaniu korygującym** – rozumie się przez to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;

25. **Działaniu zapobiegawczym** – rozumie się przez to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.

3. Wprowadzenie

Polityka Ochrony Danych Osobowych określa reguły przetwarzania danych osobowych oraz sposobów ich zabezpieczenia, jako zestaw praw, zasad i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji danych w firmie Metal-Fach Jacek Kucharewicz.

Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.

Niniejszy dokument jest zgodny z obowiązującymi przepisami prawa, a w szczególności z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz RODO.

Na podstawie przeprowadzonej analizy ryzyka utraty danych osobowych, poziom zagrożenia określono jako podstawowy.

4. Cele Polityki Ochrony Danych Osobowych

Celem Polityki Ochrony Danych Osobowych jest określenie oraz wdrożenie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w firmie „Metal-Fach Jacek Kucharewicz", a w szczególności:

1. zapewnienie spełnienia wymagań prawnych;
2. zapewnienie poufności, integralności oraz rozliczalności danych osobowych przetwarzanych w firmie;
3. podnoszenie świadomości osób przetwarzających dane osobowe;
4. zaangażowanie osób przetwarzających dane osobowe firmy w ich ochronę.

5. Inspektor Ochrony Danych (IOD)

1. Administrator Danych Osobowych powołuje Inspektora Ochrony Danych. Powołanie następuje na podstawie pisemnego powołania (wzór powołania stanowi załącznik Z1-PODO do niniejszej PODO).
2. Administrator Danych Osobowych może powołać zastępców Inspektora Ochrony Danych.
3. Administrator Danych Osobowych udziela pełnomocnictwa Inspektorowi Ochrony Danych do nadawania uprawnień do przetwarzania danych osobowych.

4. Rolą Inspektora Ochrony danych jest nadzorowanie przestrzegania zasad oraz stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w firmie „Metal-Fach Jacek Kucharewicz".

5. Do zadań Inspektora Ochrony Danych należy:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania RODO (Rozporządzenie Parlamentu Europejskiego i Rady 2016/679), innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Dodatkowo zadaniem IOD jest prowadzenie rejestru czynności przetwarzania danych osobowych, a także rejestru umów powierzenia danych.

6. ADO może powierzyć IOD wykonywanie innych obowiązków, które nie naruszają prawidłowego wykonywania zadań określonych w pkt 4-5.

6. Osoby upoważnione do przetwarzania danych osobowych

1. Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

- zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Ochrony Danych Osobowych i Instrukcji Zarządzania Systemami Informatycznymi;
- stosowanie się do zaleceń IOD;
- przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;
- niezwłoczne informowanie IOD o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w firmie;
- ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;

- korzystanie z systemów informatycznych firmy w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
- bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
- zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

7. Podstawowe zasady ochrony danych osobowych

1. Wszystkie dane osobowe w firmie należy przetwarzać zgodnie z obowiązującymi przepisami prawa.
2. W stosunku do osób, których dane osobowe są przetwarzane, należy spełnić obowiązek informacyjny wynikający z przepisów u.o.d.o..
3. Zebrane dane osobowe należy przetwarzać dla oznaczonych i zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami.
4. Należy zadbać, aby przetwarzanie danych osobowych odbywało się zgodnie z zasadami dotyczącej merytorycznej poprawności oraz adekwatnie do celów w jakich zostały zebrane.
5. Dane osobowe w firmie można przetwarzać nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania.
6. Należy zapewnić poufność, integralność oraz rozliczalność danych osobowych przetwarzanych w firmie.
7. Przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane osobom, których dane dotyczą, osobom upoważnionym do przetwarzania danych osobowych, podmiotom którym przekazano dane na podstawie umowy powierzenia oraz organom państwowym lub organom samorządu terytorialnego w związku z prowadzonym postępowaniem.
8. Przetwarzanie danych osobowych w firmie może odbywać się zarówno w systemach informatycznych, jak i w formie tradycyjnej: kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
9. W zakresie danych osobowych przetwarzanych w innych systemach niż informatyczne, obowiązują nadal dotychczasowe przepisy o tajemnicy służbowej, obiegu i zabezpieczaniu dokumentów służbowych.
10. Wszystkim osobom, których dane są przetwarzane przysługuje prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania, usunięcia jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.

8. Upoważnienie do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych i obsługi zbiorów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik Z2-PODO) wydane przez Administratora Danych Osobowych lub Inspektora Ochrony Danych oraz złożyły stosowne oświadczenie dot. właściwej realizacji przepisów u.o.d.o. (wzór oświadczenia stanowi załącznik Z3-PODO).

2. IOD w imieniu ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych (wzór ewidencji stanowi załącznik Z4-PODO).

9. Powierzenie przetwarzania danych osobowych

1) Administrator Danych Osobowych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania.

2) W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim cel i zakres przetwarzania danych osobowych. Wykaz zawartych umów powierzenia prowadzi IOD.

10. Udostępnianie danych osobowych

Udostępnienie danych osobowych w firmie dopuszcza się na podstawie jednej z podstaw prawnych określonych w u.o.d.o. lub na podstawie przepisów innych ustaw.

IOD prowadzi ewidencję udostępniania danych osobowych instytucjom i osobom spoza firmy (wzór ewidencji stanowi załącznik Z5-PODO).

11. Przekazywanie danych osobowych poza Polskę

1. Administrator Danych Osobowych może przekazywać dane osobowe do:
    - państw Europejskiego Obszaru Gospodarczego;
    - pozostałych państw (państwa trzecie).

2. Przekazywanie danych osobowych w ramach EOG traktuje się tak, jakby były przetwarzane na terenie Polski.

3. W przypadku przekazywania danych osobowych do państwa trzeciego, należy spełnić jeden z warunków:

- państwo docelowe daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązuje na terytorium Rzeczypospolitej Polskiej;
- gdy przesyłanie danych osobowych wynika z obowiązku nałożonego przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej;
- na przekazanie danych osobowych wyrazi zgodę UODO.

12. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

IOD odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz budynków, pomieszczeń lub części pomieszczeń tworzący obszar, w którym przetwarzane są dane osobowe zarówno w formie papierowej jak i elektronicznej.

Aktualny wykaz obszarów przetwarzania danych osobowych zawarto w załączniku Z6-PODO.

13. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

IOD odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz wszystkich zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Aktualny wykaz zbiorów danych osobowych zawarto w załączniku Z7-PODO.

14. Opis struktury zbiorów danych osobowych

IOD odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis struktury zbiorów danych osobowych przetwarzanych w firmie.

Aktualny opis struktury zbiorów danych osobowych zawarto w załączniku Z8-PODO.

15. Opis sposobu przepływu danych pomiędzy poszczególnymi systemami

IOD odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis sposobu przepływu danych pomiędzy poszczególnymi systemami.

Aktualny opis sposobu przepływu danych zawarto w załączniku Z9-PODO.

16. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

IOD odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej określone środki techniczne i organizacyjne niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Aktualny opis stosowanych środków technicznych i organizacyjnych zawarto w załączniku Z10-PODO.

17. Przepisy karne i porządkowe

Przepisy karne i porządkowe reguluje:

- ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000) – art. 102-108;
- ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. z 1997 r., Nr 88, poz. 553, z późn. zm.) - art. 266;
- ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 1998 r., Nr 21, poz. 94, z późn. zm.) - art. 52 oraz art. 108.

18. Postanowienia końcowe

W sprawach nieuregulowanych w niniejszej Polityce Ochrony Danych Osobowych mają zastosowanie przepisy ustawy z dnia 10 maja 2018 r., o ochronie danych osobowych (t.j. Dz.U. z 2018 r., poz. 1000) oraz przepisy wykonawcze do tej Ustawy.

Sposób postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, określono w procedurze postępowania, stanowiący załącznik nr 12 do PODO, a taki fakt odnotowuje się w rejestrze incydentów i zdarzeń, stanowiący załącznik nr 11 do PODO.

19. Załączniki

1. Z1-PODO – Powołanie na stanowisko Inspektora Ochrony Danych;
2. Z2-PODO– Upoważnienie do przetwarzania danych osobowych;
3. Z3-PODO – Oświadczenie dot. właściwej realizacji przepisów u.o.d.o.;
4. Z4-PODO – Ewidencja osób upoważnionych do przetwarzania danych osobowych;
5. Z5-PODO – Ewidencja udostępniania danych osobowych;
6. Z6-PODO – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
7. Z7-PODO – Wykaz zbiorów danych osobowych wraz ze skazaniem programów zastosowanych do przetwarzania tych danych;
8. Z8-PODO – Opis struktury zbiorów danych osobowych;
9. Z9-PODO – Opis sposobu przepływu danych pomiędzy poszczególnymi systemami;
10. Z10-PODO – Opis stosowanych środków technicznych i organizacyjnych;
11. Z11-PODO – Rejestr incydentów i zdarzeń.
12. Z12-PODO – Procedura postępowania w przypadku naruszenia bezpieczeństwa Danych Osobowych