POLITYKA BEZPIECZEŃSTWA

WYKAZ ZAŁĄCZNIKÓW:

* WZÓR UPOWAŻNIENIA I OŚWIADCZENIA DOT. PRZETWARZANIA DANYCH
* WYKAZ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH
* WYKAZ OBSZARÓW PRZETWARZANIA DANYCH OSOBOWYCH
* WYKAZ ZBIORÓW DANYCH OSOBOWYCH
* OPIS STRUKTURY ZBIORÓW
* OPIS SPOSOBU PRZEPŁYWU DANYCH
* REJESTR CZYNNOŚĆI PRZETWARZANIA DANYCH
* REJESTR NARUSZEŃ

**Administrator danych**:

Janusz Diaconescu **DIACO TECHNOLOGIA-PROJEKT Janusz Diaconescu**

ul. Blacharska 26/7, 53-206 Wrocław

NIP: 6131389993, REGON: 021913721

 pieczęć firmowa podpis/y administratora/ów danych osobowych data

Wstęp

 Stosownie do art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883, z późn, zm.), zwanej dalej ustawą, administrator danych osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. W tym celu administrator prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki zapewniające należytą ochronę.

 Zgodnie z art. 38 ustawy administrator zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Polityka bezpieczeństwa stanowi wykonanie obowiązku, o którym mowa w § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 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. Nr 100, poz. 1024, z późn. zm.).

Rozdział 1

Postanowienia ogólne

Ilekroć w Polityce bezpieczeństwa jest mowa o:

1. **administratorze danych** – rozumie się przez to Janusza Diaconescu, prowadzącego działalność gospodarczą pod firmą **DIACO TECHNOLOGIA-PROJEKT Janusz Diaconescu,** wpisanego w Centralnej Ewidencji i Informacji o Działalności Gospodarczej, posiadającego adres miejsca głównego wykonywania działalności i adres do doręczeń: ul. Blacharska 26/7, 53-206 Wrocław, NIP: 6131389993, REGON: 021913721,
2. **administratorze systemu** – rozumie się przez to rozumie się przez to Janusza Diaconescu, prowadzącego działalność gospodarczą pod firmą **DIACO TECHNOLOGIA-PROJEKT Janusz Diaconescu,** wpisanego w Centralnej Ewidencji i Informacji o Działalności Gospodarczej, posiadającego adres miejsca głównego wykonywania działalności i adres do doręczeń: ul. Blacharska 26/7, 53-206 Wrocław, NIP: 6131389993, REGON: 021913721,
3. **analizie ryzyka** – rozumie się przez to proces mający na celu oszacowanie wagi ryzyka rozumianej jako funkcja prawdopodobieństwa wystąpienia skutku i krytyczności jego następstw dla przedsiębiorstwa,
4. **danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”), możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
5. **elektronicznym nośniku** – rozumie się przez to elektroniczne urządzenie, na którym przechowuje się dane osobowe w celu jego ponownego odtworzenia w systemie informatycznym,
6. **odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania,
7. **obszarze przetwarzania danych** – rozumie się przez to wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
8. **organie nadzorczym** – rozumie się przez to Generalnego Inspektora Ochrony Danych Osobowych,
9. **osobie możliwej do zidentyfikowania** – rozumie się przez to osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizyczne,
10. **opisie przepływu danych** – rozumie się przez to opis sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi,
11. **opisie struktury zbiorów** – rozumie się przez to opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
12. **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego,
13. **przetwarzaniu danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
14. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE. L Nr 119, str. 1),
15. **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
16. **środkach technicznych i organizacyjnych** – rozumie się przez to środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych,
17. **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883 z późn. zm.),
18. **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
19. **użytkowniku systemu** – rozumie się przez to osobę, której został przydzielony przez administratora systemu indywidualny identyfikator w systemie informatycznym w powiązaniu z niezbędnymi uprawnieniami dostępowymi w tym systemie,
20. **wykazie zbiorów** – rozumie się przez to wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
21. **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
22. **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
23. **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..

Rozdział 2

Administrator danych

1. Administrator danych jest zobowiązany w szczególności do:
2. opracowania i wdrożenia Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe,
3. stałego nadzoru nad treścią Polityki bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym,
4. wydawania i anulowania upoważnienia do przetwarzania danych osobowych osobom, które mają te dane przetwarzać (załącznik nr 1),
5. prowadzenia wykazu osób upoważnionych do przetwarzania danych osobowych (załącznik nr 2),
6. prowadzenia wykazu obszarów przetwarzania (załącznik nr 3),
7. prowadzenia wykazu zbiorów danych osobowych (załącznik nr 4),
8. prowadzenia opisu struktury zbiorów (załącznik nr 5),
9. prowadzenia opisu sposobu przepływu danych (załącznik nr 6),
10. dokonywania aktualizacji dokumentów wymienionych powyżej pod lit. a-h,
11. zgłaszania Generalnemu Inspektorowi Danych Osobowych (GIODO) zbiorów danych podlegających rejestracji,
12. wykazania przestrzegania zasad przetwarzania danych opisanych w RODO.
13. Administrator danych jest zobowiązany do przetwarzania następujących zasad przetwarzania danych osobowych:
14. zgodności z prawem: przetwarzanie danych powinno następować zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
15. ograniczenia celu: zbieranie danych powinno się odbywać w konkretnych, wyraźnych i prawnie uzasadnionych celach, dane nie powinny być przetwarzane dalej w sposób niezgodny z tymi celami (dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami),
16. minimalizacji danych: przetwarzane mogą być tylko dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
17. prawidłowości: przetwarzane mogą być tylko dane prawidłowe i w razie potrzeby uaktualniane (administrator jest zobowiązany do podjęcia należy wszelkich działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane),
18. ograniczenia przechowywania: dane powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane, dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą,
19. integralności i poufności: dane powinny być przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Rozdział 3

**Zbieranie danych osobowych**

* + 1. W przypadku zbierania danych od osób, których dane dotyczą dokonujący tej czynności zobowiązany jest do poinformowania osoby, której dane dotyczą o:
	1. swojej tożsamości i danych kontaktowych oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych swojego przedstawiciela,
	2. gdy ma to zastosowanie – danych kontaktowych inspektora ochrony danych,
	3. celach przetwarzania danych osobowych, oraz podstawie prawnej przetwarzania,
	4. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią,
	5. odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
	6. gdy ma to zastosowanie –o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
	7. okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu,
	8. prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
	9. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO – o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
	10. prawie wniesienia skargi do organu nadzorczego,
	11. tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
	12. zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO oraz – przynajmniej w tych przypadkach – o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Jeżeli administrator danych będzie planował dalsze przetwarzanie danych osobowych w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem zobowiązuje się do poinformowania osoby, której dane dotyczą, o tym innym celu oraz do udzielenia jej wszelkich innych stosownych informacji, zgodnych z RODO.

3. Jeżeli danych osobowych administrator danych nie pozyskał od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, informacje wymienione w ust. 1 powyżej, jak również informuje o źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych. Informacje te należy podać:

1. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych,
2. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą,
3. jeżeli administrator danych planuje ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

4. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

1. cele przetwarzania,
2. kategorie odnośnych danych osobowych,
3. informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4. w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
5. informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6. informacje o prawie wniesienia skargi do organu nadzorczego;
7. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
8. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

5. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

6. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

7. Prawo do uzyskania kopii, o której mowa w ust. 6 powyżej, nie może niekorzystnie wpływać na prawa i wolności innych osób.

Rozdział 4

Środki ochrony

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z  RODO. Środki te są poddawane przeglądom i na bieżąco uaktualniane.
2. Uwzględniając kategorie przetwarzanych danych oraz potencjalne zagrożenia wprowadza się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.
3. 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.
4. Administrator danych, przy określaniu sposobów przetwarzania oraz w czasie samego przetwarzania wdraża odpowiednie środki techniczne i organizacyjne, takie jak:
5. Szyfrowanie danych,
6. Pseudonimizacja danych (osoby, których dane dotyczą mają przypisane pseudonimy -loginy- za pomocą których są identyfikowani w systemie administratora danych),
7. Minimalizacja danych (aby domyślnie przetwarzane były tylko te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania).
8. W celu ochrony danych spełniono wymogi, o których mowa w art. 36–39 ustawy:
9. administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji,
10. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych,
11. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
12. została opracowana i wdrożona Polityka bezpieczeństwa,
13. została opracowana i wdrożona Instrukcja zarządzania systemem informatycznym.
14. W celu ochrony danych osobowych przeprowadzono analizę ryzyka celem zabezpieczenia przed naruszeniami praw lub wolności osób, których dane dotyczą.
15. Działalność administratora i przetwarzanie danych ma miejsce w jednej lokalizacji.
16. W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:
17. zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie – drzwi klasy C,
18. pomieszczenia, w których przetwarzane są zbiory danych osobowych, wyposażone są w system alarmowy przeciwwłamaniowy (dotyczy siedziby firmy),
19. dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, objęty jest systemem kontroli (dotyczy siedziby firmy),
20. dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych (dotyczy siedziby firmy oraz domu),
21. dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony (dotyczy siedziby firmy oraz domu),
22. dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, przez całą dobę jest nadzorowany przez służbę ochrony (dotyczy siedziby firmy oraz domu),
23. pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą wolno stojącej gaśnicy,
24. dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów,
25. niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartych w nich informacji.
26. W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
27. zastosowano kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych (logiczne zabezpieczenia przed nieuprawnionym dostępem),
28. zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego,
29. dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
30. zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych,
31. zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity,
32. użyto system Firewall do ochrony dostępu do sieci komputerowej.
33. W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:
34. zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych; w sklepie internetowym można udostępnić upoważnionym osobom tylko wybrane elementy zbiorów (np. bez dostępu do zamówień),
35. dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
36. zastosowano kryptograficzne środki ochrony danych osobowych,
37. zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego,
38. zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,
39. zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
40. W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:
41. monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
42. niedopuszczalne jest przenoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych, a za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia/przeniesienia,
43. przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem,
44. w miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy/współpracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka”, co oznacza nie pozostawianie materiałów zawierających danych.

**Rozdział 5**

**Zarządzanie ryzykiem bezpieczeństwa informacji**

1. W celu skutecznej realizacji zadań związanych z bezpieczeństwem informacji przetwarzanej w systemach informatycznych przeprowadzana jest raz w roku oraz przy każdej istotnej zmianie środowiska informatycznego analiza ryzyka.

2. Proces składa się z następujących etapów:

1. identyfikacji ryzyka,
2. szacowania ryzyka,
3. przeciwdziałania ryzyku,
4. monitorowania i raportowania ryzyka IT.

3. Wyniki analizy ryzyka stanowią podstawę zaprojektowania odpowiednich mechanizmów kontroli dla systemów informatycznych eksploatowanych w organizacji.

4. Wdrażane mechanizmy kontroli powinny być adekwatne do oszacowanego ryzyka, zidentyfikowanych zagrożeń i ich istotności, oraz muszą zapewniać efektywność ekonomiczną.

5. Kontrola adekwatności oraz sposobu funkcjonowania stosowanych mechanizmów kontroli wchodzi w skład zadań administratora systemu i przeprowadzana jest w ramach szacowania ryzyka operacyjnego.

6. Za proces analizy i szacowania ryzyka bezpieczeństwa informacji odpowiedzialny jest administrator systemu/administrator danych.

7. W celu zminimalizowania ryzyka związanego z zagrożeniami bezpieczeństwa informacji każdy użytkownik systemu informatycznego powinien być regularnie szkolony z zakresu obsługi systemu i procedur bezpieczeństwa informacji oraz właściwego używania zasobów informatycznych.

8. Za organizowanie szkoleń z zakresu obsługi systemu i procedur bezpieczeństwa informacji oraz właściwego używania zasobów informatycznych odpowiedzialny jest administrator danych.

Rozdział 6

Tryb postępowania w sytuacji naruszenia ochrony danych osobowych

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić administratorowi danych.
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych administratora danych lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:
	1. niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
	2. zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
	3. udokumentować wstępnie zaistniałe naruszenie,
	4. nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia administratora danych lub osoby upoważnionej.
3. Po przybyciu na miejsce naruszenia ochrony danych osobowych, administrator danych lub osoba go zastępująca:
	1. zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania,
	2. wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.
4. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu:
5. w przypadku naruszenia ochrony danych osobowych, administrator danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia,
6. zgłoszenie, naruszenia ochrony danych osobowych organowi nadzorczemu, musi co najmniej:
* opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
* zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
* opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
* opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
1. Administrator danych dokumentuje zaistniały przypadek naruszenia oraz sporządza sprawozdanie. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania przepisów RODO.
2. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, administrator danych zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii odtworzenia danych z zabezpieczeń) oraz zarządza termin wznowienia przetwarzania danych.
3. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
4. Zawiadomienie osoby, której dane dotyczą o naruszeniu powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej następujące informacje: imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji, możliwe konsekwencje naruszenia ochrony danych osobowych oraz środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
5. Zawiadomienie osoby, której dane dotyczą o naruszeniu nie jest wymagane, w następujących przypadkach:
6. administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
7. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
8. wymagałoby ono niewspółmiernie dużego wysiłku, w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Rozdział 7

Postanowienia końcowe

1. Wszelkie zasady opisane w Polityce bezpieczeństwa są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.
2. Administrator danych może powierzyć przetwarzanie danych innemu podmiotowi, w drodze umowy zawartej w formie pisemnej. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, zobowiązuje się on korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Podmiot przetwarzający może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie oraz jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36–39 ustawy oraz w RODO oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a ustawy oraz w RODO. W zakresie przestrzegania tych przepisów taki podmiot ponosi odpowiedzialność jak administrator danych. W przypadkach, o których mowa powyżej, odpowiedzialność za przestrzeganie przepisów ustawy i RODO spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.
3. Polityka bezpieczeństwa obowiązuje od dnia jej zatwierdzenia przez administratora danych.

Załącznik nr 1

UPOWAŻNIENIE
do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze w wersji papierowej

Niniejszym, jako Administrator Danych Osobowych, na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883, z późn, zm.), z dniem ........................ upoważniam:

1. Imię i nazwisko: …………………………………………………………………………..
2. Zbiory danych objęte zakresem upoważnienia: klienci, potencjalni klienci, dostawcy, reklamacje, itd.
3. Systemy przetwarzania danych, do których ma dostęp osoba upoważniona: ………………………………………………………………………………………………………..
4. Osoba upoważniona posiada następujące uprawnienia\* (*niepotrzebne skreślić*):
5. Prawo do wprowadzania danych,
6. Prawo do modyfikacji danych,
7. Prawo do usuwania danych,
8. Prawo do przechowywania danych,
9. Prawo do przeglądania danych,
10. Prawo do zbierania danych,
11. Prawo do udostępniania danych,
12. Prawo do przekazywania danych,
13. Prawo do utrwalania danych,
14. Prawo do opracowywania danych.\*

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 upoważniania jest obowiązana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych Osobowych Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

1. Identyfikator osoby upoważnionej: …………………………………………………

Niniejsze upoważnienie jest ważne do odwołania, rozwiązania lub wygaśnięcia umowy o pracę, umowy zlecenia, umowy o dzieło lub innego stosunku prawnego.

*miejscowość, data podpis/y administratora/ów danych*

OŚWIADCZENIE

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883, z późn. zm.), wydanymi na jej podstawie aktami wykonawczymi oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych Osobowych Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Zobowiązuję się do:

* zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zobowiązań umownych lub obowiązków pracowniczych,
* niewykorzystywania danych osobowych w celach pozasłużbowych i pozaumownych o ile nie są one jawne,
* zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, o ile nie są one jawne,
* korzystania ze sprzętu komputerowego oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych lub zobowiązań umownych,
* wykorzystywania jedynie legalnego oprogramowania pochodzącego od administratora danych osobowych,
* należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją ochrony danych osobowych,
* korzystania z urządzeń przenośnych zgodnie z dokumentacją ochrony danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższym może być uznane przez Administratora Danych Osobowych za ciężkie naruszenie obowiązków pracowniczych lub zobowiązań umownych w rozumieniu przepisów prawa lub za naruszenie przepisów karnych ustawy o ochronie danych osobowych.

 podpis osoby upoważnionej

Załącznik nr 2

WYKAZ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwisko i Imię użytkownika** | **Identyfikator w systemie informatycznym** | **Wersja papierowa** | **Wersja elektroniczna** | **Data nadania upoważnienia** | **Data odebrania upoważnienia** | **Lokalizacja****(stanowisko lub miejsce pracy)** |
| 1. | Magdalena Diaconescu |  | Tak | Tak |  |  | ul. Grabiszyńska 269/7Wrocław 53-234 |
| 2. |  |  | Nie | Nie |  |  | ul. Blacharska 26/7Wrocław 53-206 |
| 3. |  |  | Nie | Nie |  |  |  |
| 4. |  |  | Nie | Nie |  |  |  |

Dane aktualne na dzień: Podpis/y administratora/ów danych:

Załącznik nr 3

WYKAZ OBSZARÓW PRZETWARZANIA DANYCH OSOBOWYCH

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Lokalizacja** | **Środki ochronyfizycznej danych** | **Środki sprzętowe infrastruktury informatyczneji telekomunikacyjnej** | **Środki ochrony w ramach narzędzi programowych i baz danych** | **Środki organizacyjne** |
| 1. | ul. Blacharska 26/7Wrocław 53-206 |  |  |  |  |
| 2. | ul. Grabiszyńska 269/7Wrocław 53-234 |  |  |  |  |
| 3. |  |  |  |  |  |

 **Legenda:**

**Skróty oznaczenia środków ochrony fizycznej danych:**

DZ – drzwi zwykłe (niewzmacniane, nie przeciwpożarowe)

DO – drzwi o podwyższonej odporności ogniowej >= 30 min.

DW – drzwi o podwyższonej odporności na włamanie – drzwi klasy C

KR – okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej

SA – system alarmowy przeciwwłamaniowy

SK – system kontroli dostępu

SM – system monitoringu z zastosowaniem kamer przemysłowych

SO – obszar nadzorowany przez służbę ochrony

SC – obszar nadzorowany przez służbę ochrony (całodobowo)

ZS – zamknięta niemetalowa szafa

ZM – zamknięta metalowa szafa

KP – zamknięty sejf lub kasa pancerna

KZS – kopia zapasowa przechowywana w zamkniętej niemetalowej szafie

KZM – kopia zapasowa przechowywana w zamkniętej metalowej szafie

KZP – kopia zapasowa przechowywana w zamkniętym sejfie lub kasie pancernej

KT – dane przechowywane w kancelarii tajnej

PPOŻ – system przeciwpożarowy i/lub wolno stojąca gaśnica

NIS – niszczarki do dokumentów

**Skróty oznaczenia środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej:**

SL – komputery połączone z lokalną siecią komputerową

UPS – zastosowano UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną

BIOS – zastosowano hasło BIOS

IH – zastosowano identyfikator użytkownika oraz hasło

TOK – zastosowano karty procesorowe oraz kod PIN lub token

BIO – zastosowano uwierzytelnienie z wykorzystaniem technologii biometrycznej

AUT – zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii

HZ – zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł

RD – zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych

KRT – zastosowano środki kryptograficznej ochrony danych w teletransmisji

UT – zastosowano mechanizm uwierzytelnienia przy dostępie do środków teletransmisji

CALL – zastosowano procedurę oddzwonienia (callback) przy transmisji za pośrednictwem modemu

MD – zastosowano macierz dyskową

ANW – zastosowano program antywirusowy

FW – zastosowano system Firewall przy dostępie do sieci komputerowej

IDS – zastosowano system IDS/IPS

**Skróty oznaczenia środków ochrony w ramach narzędzi programowych i baz danych:**

REJ – zastosowano rejestrację zmian wykonywanych na poszczególnych elementach zbioru

DOS – określono prawa dostępu do wskazanego zakresu danych

PIH – zastosowano identyfikator użytkownika oraz hasła

PTOK – zastosowano karty procesorowe oraz kod PIN lub token

PBIO – zastosowano technologię biometryczną

PRD – zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych

PZH – zastosowano okresową zmianę haseł dostępu

PKRY – zastosowano kryptograficzne środki ochrony danych

WYG – zainstalowano wygaszacze ekranów

BLOK – zastosowano automatyczną blokadę dostępu w przypadku dłuższej nieaktywności pracy użytkownika

**Skróty oznaczenia środków organizacyjnych:**

OZ – osoby upoważnione zostały zaznajomione z przepisami o ochronie danych

SZ – osoby upoważnione zostały przeszkolone z zabezpieczeń systemu informatycznego

OP – osoby upoważnione zostały zobowiązane do zachowania danych w poufności

PE – zastosowano politykę czystego ekranu

KZ – kopia zapasowa danych jest przechowywana w innym pomieszczeniu niż oryginał

Dane aktualne na dzień: Podpis/y administratora/ów danych:

Załącznik nr 4

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa zbioru danych** | **Program przetwarzający** | **Lokalizacja** | **Podstawa prawna przetwarzania danychw zbiorze** |
| 1 | Klienci sklepu internetowego [www.studiodiaco.pl](http://www.studiodiaco.pl) oraz Klienci sklepu internetowego www.farbygalvi.pl | Wersja elektroniczna – oprogramowanie sklepu Woocommerce, program do fakturowania fakturex.pl | ul. Blacharska 26/7Wrocław 53-206ul. Grabiszyńska 269/7Wrocław 53-234 | Art. 6 ust. 1 lit. b RODO – przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy |
| 2 | Potencjalni klienci kontaktujący się za pośrednictwem formularzy kontaktowych | Wersja elektroniczna oprogramowanie sklepu Woocommerce | ul. Blacharska 26/7Wrocław 53-206ul. Grabiszyńska 269/7Wrocław 53-234 | Art. 6 ust. 1 lit. a RODO – osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów |
| 3  | Dostawcy | Wersja elektroniczna | ul. Blacharska 26/7Wrocław 53-206ul. Grabiszyńska 269/7Wrocław 53-234 | Art. 6 ust. 1 lit. b RODO – przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy |
| 4 | Klienci otrzymujący informację handlową | Wersja elektroniczna | ul. Blacharska 26/7 Wrocław 53-206ul. Grabiszyńska 269/7Wrocław 53-234 | Art. 6 ust. 1 lit. a RODO – osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów |
| 5 | Użytkownicy konta | Wersja elektroniczna oprogramowanie sklepu Woocommerce | ul. Blacharska 26/7 Wrocław 53-206ul. Grabiszyńska 269/7Wrocław 53-234 | Art. 6 ust. 1 lit. a RODO – osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów |
| 6 | Reklamacje | Wersja elektroniczna | ul. Blacharska 26/7 Wrocław 53-206ul. Grabiszyńska 269/7Wrocław 53-234 | Art. 6 ust. 1 lit. c RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze – wypełnienie obowiązków wynikających z Kodeksu cywilnego (przepisy o rękojmi) |
| 7 | Pracownicy | Wersja papierowa z wykorzystaniem komputera, wersja elektroniczna | ul. Blacharska 26/7 Wrocław 53-206ul. Grabiszyńska 269/7Wrocław 53-234 | Art. 6 ust. 1 lit. b RODO – przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, Art. 6 ust. 1 lit. c RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze – wypełnienie obowiązków wynikających z prawa pracy |

Dane aktualne na dzień: Podpis/y w imieniu administratora/ów danych:

Załącznik nr 5

OPIS STRUKTURY ZBIORÓW

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa zbioru danych** | **Wersja papierowa** | **System informatyczny** | **Zawartość pól informacyjnych i powiązania pomiędzy nimi** |
| Klienci sklepu internetowego [www.studiodiaco.pl](http://www.studiodiaco.pl) oraz Klienci sklepu internetowego www.farbygalvi.pl  | Tak | Tak | dane adresowe klienta: [**identyfikator klienta**, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), nazwa i siedziba firmy, numer NIP, adres e-mail, numer telefonu, adres dostawy] + zamówienia klienta: [**identyfikator zamówienia**, zakres zamówienia, wartość zamówienia, data zamówienia, data realizacji, metoda płatności, metoda dostawy] + sprzedawane towary:  [**identyfikator towaru**, nazwa towaru, numer katalogowy, nazwa producenta, opis, specyfikacja, cena jednostkowa] |
| Potencjalni klienci kontaktujący się za pośrednictwem formularzy kontaktowych | Nie | Tak | Imię i nazwisko, adres e-mail, telefon + treść wiadomości + odpowiedź na wiadomość |
| Dostawcy | Tak | Tak | dane adresowe: imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), adres e-mail, telefon, nazwa i siedziba firmy, numer identyfikacji podatkowej (NIP), REGON, KRS + umowa zawarta z dostawcą + zlecenia/zamówienia realizowane przez dostawcę |
| Klienci otrzymujący informację handlową | Nie | Tak | adres e-mail klienta [**identyfikator klienta**, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania) + treść wiadomości zawierającej informację handlową |
| Użytkownicy konta | Nie | Tak | dane adresowe użytkownika: [**identyfikator**, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), nazwa i siedziba firmy, numer NIP, adres e-mail, numer telefonu, adres dostawy] + zamówienia klienta: [**identyfikator zamówienia**, zakres zamówienia, wartość zamówienia, data zamówienia, data realizacji, metoda płatności, metoda dostawy] + sprzedawane towary:  [**identyfikator towaru**, nazwa towaru, numer katalogowy, nazwa producenta, opis, specyfikacja, cena jednostkowa] |
| Reklamacje | Nie | Tak | dane adresowe klienta: [**identyfikator klienta**, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), nazwa i siedziba firmy, numer NIP, adres e-mail, numer telefonu, adres dostawy] + zamówienia klienta: [**identyfikator zamówienia**, zakres zamówienia, wartość zamówienia, data zamówienia, data realizacji, metoda płatności, metoda dostawy] + sprzedawane towary:  [**identyfikator towaru**, nazwa towaru, numer katalogowy, nazwa producenta, opis, specyfikacja, cena jednostkowa] + termin złożenia reklamacji + decyzja dotycząca reklamacji |
| Pracownicy | Tak | Tak | …………………. |

Dane aktualne na dzień: Podpis/y w imieniu administratora/ów danych: Załącznik nr 6

OPIS SPOSOBU PRZEPŁYWU DANYCH

|  |  |  |
| --- | --- | --- |
| **Zbiór danych osobowych** | **Rodzaj systemu/programu/procesora** | **Sposób przesyłania danych osobowych** |
| Klienci sklepu internetowego [www.studiodiaco.pl](http://www.studiodiaco.pl) oraz Klienci sklepu internetowego www.farbygalvi.pl | Manualny/półautomatyczny/automatyczny\*hosting: HEADWAY Sp. z o. o.oprogramowanie sklepu: Woocommercebiuro rachunkowe: IZABELA MAGNOWSKAwysyłka towarów sklepu internetowego [www.farbygalvi.pl](http://www.farbygalvi.pl): Sendit S.A.wysyłka towarów sklepu internetowego [www.studiodiaco.pl](http://www.studiodiaco.pl): InPost Paczkomaty Sp. z o.o., DPD Strefa Paczki Sp. z o.o. operator płatności: Krajowy Integrator Płatności S.A.zarządzanie stroną [www.studiodiaco.pl](http://www.studiodiaco.pl): HEADWAY Sp. z o. o.program do fakturowania: Fakturex.pl | Przepływ danych:  |
| Potencjalni klienci kontaktujący się za pośrednictwem formularzy kontaktowych | Manualny~~/~~półautomatyczny~~/~~automatyczny\*hosting: HEADWAY Sp. z o. o.oprogramowanie sklepu: Woocommerce | Przepływ danych:  |
| Dostawcy | Manualny/półautomatyczny/automatyczny~~\*~~biuro rachunkowe: IZABELA MAGNOWSKAprogram do fakturowania: Fakturex.pl | Przepływ danych:  |
| Klienci otrzymujący informację handlową | ~~Manualny~~/półautomatyczny/~~automatyczny~~\*hosting: HEADWAY Sp. z o. o.oprogramowanie sklepu: Woocommerce | Przepływ danych: |
| Użytkownicy konta | ~~Manualny/półautomatyczny/~~automatyczny\*hosting: HEADWAY Sp. z o. o.Woocommerce  | Przepływ danych:  |
| Reklamacje | Manualny/~~półautomatyczny/automatyczny\*~~ | Nie istnieje bezpośredni przepływ danych |
| Pracownicy  | Manualny/półautomatyczny/automatyczny\*biuro rachunkowe: IZABELA MAGNOWSKA | ……………………………………… |

Dane aktualne na dzień: Podpis/y w imieniu administratora/ów danych……………………………

 \*niepotrzebne skreślić

Załącznik nr 7

REJESTR CZYNNOŚĆI PRZETWARZANIA DANYCH

|  |  |
| --- | --- |
| Nazwa administratora | Dane kontaktowe |
| Janusz Diaconescu | ul. Blacharska 26/7 53-206 Wrocław  |
| Nazwa współadministratorów | Dane kontaktowe |
| ---------------------------------------------------- | ---------------------------------------------------- |
| Nazwa przedstawiciela administratora | Dane kontaktowe |
| ---------------------------------------------------- | ---------------------------------------------------- |
| Imię i nazwisko inspektora ochrony danych | Dane kontaktowe |
| ---------------------------------------------------- | ---------------------------------------------------- |
| cele przetwarzania | kategorie osób, których dane dotyczą | kategorie danych osobowych | kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione | nazwa państwa trzeciego, któremu dane osobowe są przekazywane | planowany termin usunięcia poszczególnych kategorii danych | opis technicznych i organizacyjnych środków bezpieczeństwa |
| zarządzanie kontem (usługą elektroniczną konta) | użytkownicy konta | imię i nazwisko,adres zamieszkania,nr telefonu,adres e-mail | Firma zarządzająca stronami sklepów internetowych | Nie dotyczy | niezwłocznie po rezygnacji z usługi konta |  |
| sprzedaż  | klienci | imię i nazwisko,adres dostawy,nr telefonu,adres e-mail | Biuro rachunkowe, Firma zarządzająca stronami sklepów internetowych, hostingodawca, operator płatności, firma kurierska | Nie dotyczy | 5 lat |  |
| reklamacje  | klienci | imię i nazwisko,adres dostawy,nr telefonu,adres e-mail | ……………. | Nie dotyczy | 2 lata |  |
| ewidencja umów z dostawcami/kontrahentami | dostawcy | imię i nazwisko,nazwa firmy,adres siedziby/prowadzenia działalności,nr telefonu,adres e-mail,NIP/KRS/REGON | Biuro rachunkowe | Nie dotyczy | 10 lat |  |
| przesyłanie informacji handlowej | osoby, które wyraziły zgodę na przesyłanie informacji handlowej  | Imię i nazwisko,Adres e-mail | Firma zarządzająca stronami sklepów internetowych, hostingodawca | Nie dotyczy | niezwłocznie po rezygnacji z przesyłania informacji handlowej |  |
| Cele marketingowe, promocja produktów  | Klienci, potencjalni klienci | mię i nazwisko,Adres e-mail, nr telefonu | ……………. | Nie dotyczy | niezwłocznie po rezygnacji z przesyłania wiadomości promocyjnych/marketingowych |  |
| pracownicy – spełnienie wymogów przewidzianych w przepisach prawa | pracownicy | ……………. | Biuro rachunkowe | Nie dotyczy | 50 lat |  |

Załącznik nr 8

**REJESTR NARUSZEŃ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rodzaj naruszenia | Obowiązek zgłoszenia organowi nadzorczemu | Obowiązek zawiadomienia osoby, której dane dotyczą | Okoliczności naruszenia  | Skutki naruszenia | Podjęte działania zaradcze/ prewencyjne |
| Art. ……. RODO  | TAK/NIE\* | TAK/NIE\* | Dnia …….  | *Przypadkowe zniszczenie danych osobowych zawartych w …..* | *Poinformowanie organu nadzorczego/ poinformowanie osoby, której dane dotyczą/ dodatkowe przeszkolenie pracowników w zakresie znajomości RODO/ przyjęcie następującej procedury: ………….\** |

\*niepotrzebne skreślić