JAK WDROŻYĆ RODO– KROK PO KROKU

Jeżeli przetwarzasz dane osobowe, w tym przede wszystkim dane wrażliwe RODO Cię dotyczy.

Pamiętaj! RODO to **nie potwór**. Usiądź wygodnie i zastanów się na tym, co dzieje się z danymi osobowymi w Twojej firmie/działalności. Pamiętaj też, że nie musisz oficjalnie prowadzić firmy zarejestrowanej w CEIDG, żeby stosować obowiązki z RODO.

Wykonując poszczególne zadania z listy miej na uwadze główne zasady RODO. Zasad tych jest około 10, ale ja skróciłam je do trzech i zrobiłam z tego

Zasadę 3xM:
MYŚL / MINIMALIZUJ / MONITORUJ

Z kolei, te standardowe zasady RODO umieściłam na czytelnej ulotc

którą również Wam udostępniam

(gdyby ktoś nie miał okazji zobaczyć jej wcześniej).

Co oznacza zasada 3xM?

- ✓ Najpierw **myśl** co dzieje się z danymi osobowymi w Twojej firmie, jak je przetwarzasz, gdzie one lądują, jak są zabezpieczone.
- ✓ Później, **minimalizuj** liczbę tych danych, ograniczając je tylko do niezbędnych. Nie gromadź „na zapas", a bo „kiedyś się przyda".
- ✓ A gdy już wszystko masz opanowane w zakresie ich ochrony – **monitoruj**, czyli sprawdzaj na bieżąco, czy nie doszły Ci nowe dane, czy też nie warto byłoby zmienić środki ochrony ze względu na ważność tych danych.

I pamiętaj jeszcze o jednej ważnej rzeczy – ROZLICZALNOŚĆ!
Nie wystarczy, że powiesz, iż wdrożyłaś RODO u siebie! Musisz się z tego rozliczyć. Najlepszym sposobem na to jest posiadanie DOKUMENTACJI.

Zasad RODO trzeba tak samo przestrzegać, jak każdych innych przepisów tego rozporządzenia albo innych przepisów prawnych!

To ZACZYNAMY!

I. IDENTYFIKACJA DANYCH OSOBOWYCH W FIRMIE

Wypełnij poniższą tabelę. Pomoże Ci ona uświadomić sobie, co dzieje się u Ciebie z danymi, w jakim celu, na jakiej podstawie je zbierasz (czy w ogóle jakaś jest), gdzie te dane się znajdują oraz kto jeszcze ma do nich dostęp. Zrób po prostu krótki audyt.

Lp.	W jakim celu przetwarzam dane? Z jakim działaniem jest to związane?	Jakie dane przetwarzam w tym celu?	Na jakiej podstawie mogę zbierać lub przechowywać te dane?	W jakiej formie te dane są dostępne? W jakich systemach IT?	Jaka firma wykonuje dla mnie zadania, do których niezbędny jest dostęp do tych danych?
1.	*Np. Wysyłka newslettera*	*Np. imię, nazwisko, e-mail*	*Zgoda osoby*	*Elektroniczna System do wysyłki mailingu*	*Mailchimp*
2.	*Np. Kontakt z Klientem w sprawie usługi*	*Imię, nazwisko, numer telefonu*	*W celu realizacji umowy (usługi)*	*Papierowa (kalendarz fizyczny)*	*Nie dotyczy*
3.	*Np. Przekazywanie danych księgowej*				
4.	*Np. Przekazywanie danych kurierowi*				
5.	*Np. Rekrutacja pracowników*				
6.	*Np. Konsultacja online z klientem*				
7.	*Np. Grupa na Facebooku _____ [nazwa]*				

Jeśli uzupełnisz powyższe dane rzetelnie, bez problemu wypełnisz rejestr czynności przetwarzania, o którym napiszę dalej.

Już na tym etapie, dobrze byłoby gdybyś ze swojej dotychczasowej dokumentacji, usunęła wszelkie pozostałości po starej ustawie z 1997 r. czy wzmianki o GIODO (obecnie mamy PUODO).

Mam na myśli dokumenty, ale i wszelkie inne klauzule dostępne na Twojej stronie www, blogu, czy sklepie. Jeśli je pozostawisz, będzie to wprost oznaczać, że nic w temacie RODO nie zrobiłaś i … podłożysz się organowi kontroli.

II. STWÓRZ PROCEDURY

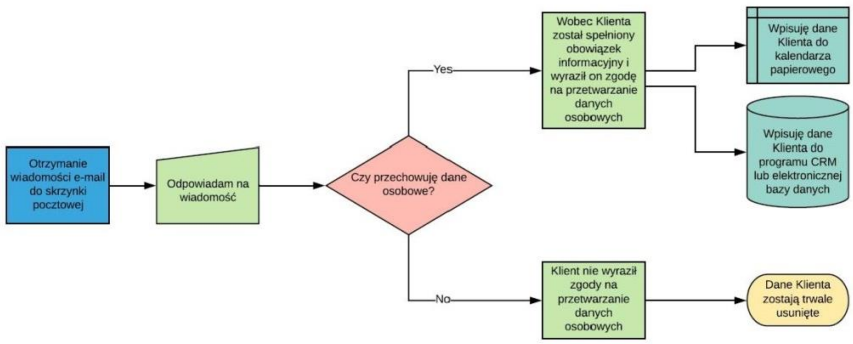
Gdy już wiesz, jak wygląda przetwarzanie poszczególnych danych u Ciebie, stwórz **PROCEDURY.**

Możesz zacząć od tego, że napiszesz, jak to wygląda obecnie. Możesz też od razu wziąć się za projektowanie „stanu docelowego", idealnego.

Po prostu, za pomocą chmurek i strzałek, rozpisz dany proces, np. klient pisze do mnie e-maila i co dzieje się dalej? Kto mu odpowiada? Osoba upoważniona czy nie? Co dzieje się z mailem? Jakie dane podaje klient i co z nimi robię? Itd.

Przykład takiej procedury poniżej.

Procedura reakcji na otrzymaną wiadomość e-mail



III. DOBIERZ ŚRODKI BEZPIECZEŃSTWA

Gdy już wiesz, jak wyglądają u Ciebie poszczególne procesy oraz zaczęłaś tworzyć procedury stanu idealnego nastawionego na ochronę danych, dobierz odpowiednie środki zabezpieczające te dane.

Następnie, opisz je w dokumentacji wewnętrznej (i zewnętrznej – jeśli jest taka potrzeba).

Tymi środkami (fizycznymi, organizacyjnymi lub technicznymi) mogą być na przykład:

- zamykana na klucz szafa (metalowa lub niemetalowa),

- system alarmowy,

- niszczarka na dokumenty,

- szyfrowanie dokumentów,

- specjalne wymagania co do hasła na komputerze,

- szyfrowanie komputera, dysków zewnętrznych, pendrive'ów z danymi,

- wygaszacz ekranu (krótki czas braku aktywności),

- odblokowywanie telefonu za pomocą odcisku palca, skanu twarzy, trudnego kodu,

- przeszkolenie pracowników,

- zobowiązanie pracowników do zachowania poufności,

Itp.

IV. ZAŁÓŻ REJESTR CZYNNOŚCI PRZETWARZANIA

Pomimo, iż ten dokument nie jest obowiązkowy dla małych firm, to jednak według mnie jest **jednym z najważniejszych dokumentów.** Jest też wskazany przez Prezesa Urzędu Ochrony Danych Osobowych jako jeden z najważniejszych dokumentów (paradoksalnie obowiązkowych).

To z tego dokumentu wynikają następujące dane:

- czynności przetwarzania,

- cel przetwarzania,

- kategorie osób, których dane dotyczą,

- kategorie odbiorców danych,

- podstawa prawna,

- źródła danych

- opis środków bezpieczeństwa,

Itp.

W celu dokładnego poznania zawartości rejestru (tak naprawdę jego poszczególnych kolumn) przeczytaj **art. 30 RODO.**

Rejestr możesz zrobić po prostu **w Excelu czy tabelce Worda.**

Przy uzupełnieniu tego dokumentu, bardzo pomocna będzie identyfikacja danych osobowych, jaką dokonałaś na samym początku. Nie pomijaj więc tamtego etapu.

V. SPRAWDŹ CZY NIE POWIERZASZ KOMUŚ SWOICH DANYCH

Pewnie słyszałaś o **tzw. umowach powierzenia?**

Są to umowy z podmiotami trzecimi, którzy otrzymują w jakiś sposób dostęp do Twoich danych (głównie dlatego, że im go dajesz w celu wykonania określonych usług/zadań).

Takimi podmiotami są na przykład:

- księgowa, kadrowa,

- informatyk, świadczący dla Ciebie usługi IT,

- usługi BHP,

- dropshipping,

- usługi hostingu,

- system do obsługi newslettera,

- wirtualna asystentka,

- agencja marketingowa lub osoba przygotowująca dla Ciebie reklamy/marketing.

Ciekawostka

Zwróć uwagę, że Poczta Polska S.A. lub firmy kurierskie wpisane do Rejestru Operatorów Pocztowych UKE (sprawdź swoją firmę w tym rejestrze) nie wymagają podpisania z nimi umowy powierzenia!

Gdy już zebrałaś wszystkie umowy powierzenia, zrób z nich **rejestr umów powierzenia** i uzupełniaj go na bieżąco. Jego też możesz wykonać w Excelu lub dokumencie Word.

VI. SPRAWDŹ CZY MUSISZ POWOŁAĆ INSPEKTORA OCHRONY DANYCH

Prawdopodobnie, nie musisz go powoływać, gdyż nie przetwarzasz danych na dużą skalę (która, co lepsze, nie wiadomo do końca co znaczy ☺).

Sprawdź ewentualnie, czy jesteś zobowiązana do jego powołania ze względu na specyfikę swojej działalności, w **art. 37 ust. 1 RODO.**

VII. KONTROLUJ SWOJĄ ODPOWIEDZIALNOŚĆ

Pamiętaj, że to głównie na Tobie jako na administratorze danych osobowych spoczywa odpowiedzialność za ich prawidłowe przetwarzanie.

To Ty poniesiesz karę, nawet jeśli będzie ona solidarna...

Nie będę Cie straszyć karami, bo możesz je „wygooglać", ale są wysokie.

VIII. DANE WRAŻLIWE – KIEDY MOŻNA JE PRZETWARZAĆ - OBOWIĄZKI

RODO w art. 6 mówi o podstawach przetwarzania danych osobowych zwykłych, a w art. 9 mówi o podstawach przetwarzania danych osobowych wrażliwych.

Zasada ogólna jest taka, że nie można przetwarzać danych wrażliwych! Wyjątki, kiedy można to robić opisane są w art. 9 ust. 2 RODO.

Więcej informacji o danych wrażliwych znajdziesz w motywach 51, 52, 53 RODO, w pozostałych przepisach RODO oraz w ustawie o ochronie danych osobowych, na stronie internetowej Urzędu Ochrony Danych Osobowych oraz na moim blogu legalnybiznesonline.pl.

Fakt przetwarzania przez Ciebie danych o zdrowiu wymaga znacznie większej ostrożności przy zabezpieczaniu danych.

Jeżeli dodatkowo **nagrywasz rozmowy** a później przechowujesz te dane to zastanów się czy rzeczywiście jest to konieczne. Z pewnością musisz przekazać klientom obowiązek informacyjny, z informacją jak długo będziesz przetwarzać te dane, co się z nimi dzieje, kto ma do nich dostęp (komu je powierzasz) i jak je chronisz.

IX. NIE PANIKUJ TYLKO DZIAŁAJ MAŁYMKI KROKAMI!

Panika w niczym nie pomaga.

Rób powoli, dokładnie, wdrażaj, a kary nie dostaniesz. Jakikolwiek Twój krok w stronę RODO to już jest dobrze!

Żeby Cię uspokoić, **weź pod uwagę te elementy:**

- prawdopodobnie karanie zacznie się od tych największych graczy na rynku, **ALE** nie wiadomo, kiedy przyjdą do Ciebie,

- oprócz wielomilionowych kar są też upomnienia, **ALE** gorsi mogą okazać się pieniacze i Ci, którzy zaczną zarabiać na „wyszukiwaniu zgodności z RODO", albo po prostu Twoi klienci, którzy przyjdą z roszczeniami.

Pamiętaj, że należy mieć na uwadze dwa obszary, jeśli chodzi o RODO:

1. **To co widać na zewnątrz,** czyli strona www (newsletter, polityka prywatności, regulamin, obowiązki informacyjne przy formularzu zapisu/komentarzach/innych formularzach/wysyłce e-maili, cookies – patrz checklista wyżej).

2. **To co jest wewnątrz Twojej działalności** – pełna dokumentacja RODO.

Co obejmuje dokumentacja?

PAKIET RODO MUST HAVE + STRONA WWW zawiera takie dokumenty jak:

- Lista kontrolna – pytania audytowe
- Identyfikacja danych osobowych w działalności z przykładami
- Rejestr czynności przetwarzania z przykładami
- Analiza ryzyka
- Rejestr naruszeń ochrony danych osobowych
- Zgłoszenie incydentu naruszenia danych osobowych – wzór według UODO
- Zgłoszenie incydentu naruszenia danych osobowych – wzór uproszczony
- Instrukcja postępowania w przypadku naruszenia zasad ochrony danych osobowych
- Polityka ochrony danych osobowych (Polityka bezpieczeństwa danych)
- Instrukcja zarządzania systemem informatycznym
- Rejestr kont, osób i systemów przetwarzających dane osobowe
- Procedura realizacji praw podmiotów danych zgodnie z RODO
- Obowiązek informacyjny – wzór – w przypadku wysyłania e-maili
- Obowiązek informacyjny – wzór – w przypadku wykonania usługi lub umowy
- **BONUS: Tablica informacyjna RODO do wywieszenia – kilka wariantów graficznych**
-

Pakiet STRONA INTERNETOWA (strona www – wizytówka), który jest dołączony do Pakietu RODO MUST HAVE, zawiera:

- Polityka prywatności i plików cookies na stronę www – uproszczona
- Klauzula informacyjna (wzór) – formularz kontaktowy
- Klauzula informacyjna (wzór) – newsletter
- Wzór checkboxa ze zgodą do wysyłki newslettera

PAKIET RODO PRACOWNIK / WSPÓŁPRACOWNIK
To pakiet dokumentów wymaganych przez RODO w sytuacji, **gdy zatrudniasz chociaż jednego pracownika albo zlecasz usługi innym przedsiębiorcom, lub freelancerom.**

PAKIET RODO PRACOWNIK / WSPÓŁPRACOWNIK zawiera takie dokumenty jak:

- Upoważnienie do przetwarzania danych osobowych
- Rejestr osób upoważnionych do przetwarzania danych osobowych
- Umowa powierzenia danych osobowych – wzór
- Rejestr umów powierzenia
- Oświadczenie o poufności dla pracownika / współpracownika
- Wzór klauzuli informacyjnej – w przypadku prowadzenia rekrutacji
- Wniosek o nadanie dostępu do systemu informatycznego
- Rejestr kont, osób i systemów przetwarzających dane osobowe

- Rejestr pomieszczeń, w których przetwarzane są dane osobowe

BONUS: Dekalog ochrony danych osobowych - kilka wariantów graficznych- do powieszenia w firmie.

Pamiętaj o tym, żeby uzupełniać ją na bieżąco.

BONUS !

RODO NA STRONIE WWW LUB BLOGU

– MINI CHECKLISTA

- ☐ Sprawdź czy pojawia się u Ciebie komunikat o ciasteczkach
- ☐ Sprawdź czy masz checkboxy przy zapisie na newsletter (wszystkie formularze),
- ☐ Checkboxy nie mogą być połączone – osobno zgoda na newsletter, na informacje handlowe (jeśli wysyłasz oferty),
- ☐ Checkboxy nie mogą być zaznaczone „z góry",
- ☐ Sprawdź czy checkboxy napisane są prosto i zrozumiale,
- ☐ Ustaw double opt-in – czyli potwierdzenie e-mailem nowego subskrybenta,
- ☐ Ustaw w automatycznej wiadomości powitalnej tzw. obowiązek informacyjny,
- ☐ Sprawdź czy Twoja polityka prywatności nie odnosi się do starej ustawy z 1997 r. lub do GIODO. Jeśli tak – wykasuj te odnośniki w każdym miejscu,
- ☐ Przygotuj politykę prywatności.

X. UWAGA – NIESPODZIANKA!

Postanowiłam zrobić coś dodatkowego dla Ciebie, skoro już tutaj jesteś! 😊 Doszedłeś do końca poradnika, a to nie lada wyczyn. W końcu poradnik jest o … RODO.

Jeśli jeszcze nie wdrożyłeś RODO i zastanawiasz się nad kupnem pakietu dokumentacji to nie zastanawiaj się dłużej.

Skorzystaj ze zniżki na Pakiet RODO MUST HAVE BASIC + PRACOWNIK/WSPÓŁPRACOWNIK – aż 20%!!

Co należy zrobić?

1. Wejdź na stronę sklepu i wrzuć produkt do koszyka: https://bazawiedzy.managerkaumow.pl/product/rodo-must-have-pracownik/
2. Wpisz kod rabatowy: **legalnawww20**
3. Opłać zamówienie.
4. Ciesz się zniżką i wdrażaj RODO!

POWODZENIA WE WDROŻENIU RODO!

Mam nadzieję, że powyższe punkty pozwolą Ci na sprawniejsze wdrożenie RODO w swojej działalności!

Jeśli masz pytania – napisz do mnie na kontakt@legalnybiznesonline.pl lub zadaj je na ***fanpage Ilona Przetacznik*** **– Legalny Biznes Online** *albo wejdź na stronę https://legalnybiznesonline.pl/*

Chcesz wiedzieć kim jestem?

Ilona Przetacznik – radca prawny. Uczy małe firmy i biznesy online, na co zwrócić uwagę podpisując umowy oraz pokazuje legalną stronę ich prowadzenia. Bez zbędnego "ą - ę" szerzy wiedzę o RODO, m.in. poprzez bezpłatne LIVE'y #LegalnaKawa na swoim fanpage i blogu. Wdraża RODO, konsultuje i sporządza umowy. Prowadzi konkretne szkolenia i warsztaty. Zarządza blogiem legalnybiznesonline.pl i grupą #Legalny Biznes Online. Działa pro bono w Fundacji Prawo dla Mam.