Podstawowe informacje dla Klientów Biura Rachunkowego BATAX dotyczące ochrony danych osobowych po 25 maja 2018 roku:

OGÓLNIE O RODO

- **Co to jest RODO:**

RODO to skrót oznaczający 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 (rozporządzenie ogólne o ochronie danych), który zastępuje dotychczasowa dyrektywę 95/46/WE.

Ważne: RODO będzie bezpośrednio obowiązywać, będzie bezpośrednio stosowane i bezpośrednio skuteczne w każdym porządku prawnym krajów UE, w tym Polsce. Oznacza to, że (z bardzo niewielkimi wyjątkami), całe prawo ochrony danych osobowych znajdziemy bezpośrednio w tekście RODO. Tym samym RODO zastąpi obowiązującą obecnie ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych. W dokumentach anglojęzycznych Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. jest określane skrótem GDPR, od angielskiej nazwy: General Data Protection Regulation.

- **Od kiedy:**

RODO będzie stosowane od 25 maja 2018 r. To właśnie do tej daty wszystkie podmioty, które podlegają RODO, powinny być gotowe do jego stosowania. Nie ma już żadnego dodatkowego okresu przejściowego.

- **Kto podlega:**

RODO podlega działalność gospodarcza prowadzona w Unii Europejskiej w jakiejkolwiek formie prawnej: spółka, jednoosobowa działalność gospodarcza czy nawet oddział w Unii Europejskiej przedsiębiorcy mającego siedzibę poza Unią: słowem – każdy przedsiębiorca. Nie ma znaczenia narodowość osób, których dane osobowe są przetwarzane ani to, gdzie przetwarzane są dane osobowe (czyli np.: gdzie znajdują się serwery).RODO znajduje zastosowanie również, gdy podmioty spoza Unii Europejskiej oferują swoje towary i usług osobom przebywający w Unii.

Regulacje RODO **nie znajdują zastosowania** w odniesieniu do działalności osobistej lub domowej. Oznacza to, że osoba fizyczna prowadząca działalność gospodarczą musi stosować RODO do danych osobowych swoich klientów czy pracowników, ale nie stosuje RODO do danych przetwarzanych w celach czysto prywatnych, np. do danych adresatów kartek świątecznych.

Podstawa prawna: art. 3 RODO.

- **Co podlega:**

RODO stosuje się do przetwarzania danych osobowych, czyli jakichkolwiek operacji wykonywanych na danych osobowych, np.:

- zbieranie danych,
- przechowywanie danych,
- usuwanie danych,
- opracowywanie danych,
- udostępnianie danych.

Ważne: RODO obejmuje wszelkie czynności, które mają za przedmiot dane osobowe – czyli nie tylko np. usługę archiwizowania dokumentów, ale także wszelkie usługi, w których dochodzi do zbierania danych osobowych. Dlatego RODO powinni stosować:

- przedsiębiorcy zajmujący się przetwarzaniem danych, jak np.: archiwizacja danych, niszczenie dokumentów, usługi kurierskie itp.,
- przedsiębiorcy, którzy przetwarzają dane osobowe przy okazji świadczenia innych usług, jak np.: pośrednicy ubezpieczeniowi, agenci biur podróży, księgowi, sklepy internetowe, zarządcy nieruchomości itp.

Podstawa prawna: art. 3, 4 pkt 2 RODO

- **Kary za nieprzestrzeganie:**

Za nieprzestrzeganie zapisów RODO podmiot może zostać ukarany karą:

- do 4% swojego rocznego globalnego obrotu

lub

- w wysokości 20 milionów euro.

To maksymalna kara, jaką może zostać nałożona za najpoważniejsze naruszenia, takie jak:

- brak uzyskania dostatecznej zgody na przetwarzanie danych osobowych,
- naruszenie podstawowych wymogów privacy by design.

Za drobniejsze przewinienia na przedsiębiorstwo może zostać nałożona kara w wysokości 2% jego rocznego globalnego obrotu, np. za:

- naruszenie obowiązku rejestrowania czynności przetwarzania,
- niezgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu,
- niedokonanie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

Ważne: zasady te mają zastosowanie zarówno do administratorów, jak i procesorów

DANE OSOBOWE

- **Co to są dane osobowe:**

Dane osobowe to wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba zidentyfikowana to taka osoba, której tożsamość znamy, którą możemy wskazać spośród innych osób. Osoba możliwa do zidentyfikowania to taka osoba, której tożsamości nie znamy, ale możemy poznać, korzystając z dostępnych nam środków.

Na przykład:

- pracownik, którego dane osobowe przetwarza pracodawca – to osoba zidentyfikowana,
- potencjalny kontrahent, którego mamy tylko numer ewidencyjny w CEIDG – osoba możliwa do zidentyfikowania,
- klient sklepu internetowego, który podał swoje dane osobowe do wysyłki zamówienia – to osoba zidentyfikowana,
- nadawca listu poleconego, znany z numeru nadanej przesyłki – osoba możliwa do zidentyfikowania,
- osoba, która w formularzu kontaktowym podaje swoje imię, nazwisko i adres e-mail – to osoba zidentyfikowana.

Dane osobowe to informacje o osobach fizycznych. Osoby prawne nie mają danych osobowych – ale ich pracownicy mają dane osobowe, jak każda inna osoba fizyczna:
Na przykład:

- nazwa ABC Sp. z o. o. – nie stanowi danych osobowych tego podmiotu,
- informacja „Jan Kowalski, pracownik ABC sp. z o. o.” – może stanowić dane osobowe Jana Kowalskiego.

Na uznanie informacji za dane osobowe nie mają wpływu ani wiek, ani narodowość osoby fizycznej

Wyróżniamy:

- dane osobowe zwykłe,
- dane osobowe zaliczające się do szczególnych kategorii danych (w dotychczasowej UOD: dane wrażliwe).

Do tej drugiej kategorii danych osobowych zaliczamy dane ujawniające:

- pochodzenie rasowe lub etniczne, poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne oraz dane biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Podstawa prawna: art. 4 pkt 1, art. 9 i 10 RODO.

- **Co to jest zbiór danych osobowych:**

Zbiór danych to każdy posiadający strukturę zestaw danych o charakterze osobowym, czyli każdy uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Ważne: Zestaw danych osobowych stanowią także aplikacje składane przez przyszłych pracowników, do celów rekrutacji.

Podstawa prawna: art. 4 pkt 6 RODO.

- **Co to jest przetwarzanie danych osobowych:**

Przetwarzanie danych osobowych to bardzo ogólne sformułowanie, oznaczające jakiekolwiek operacje wykonywane na danych osobowych, takie jak:

- zbieranie danych,
- przechowywanie danych,
- usuwanie danych,
- opracowywanie danych,
- udostępnianie danych.

Jeżeli jakiś przedsiębiorca przetwarza dane osobowe, to może to robić jako jeden z dwóch kategorii podmiotów:

1. **jako administrator danych,**
2. **jako podmiot przetwarzający dane.**

✓ **Administrator danych** to taki podmiot, który decyduje o celach (po co?) i sposobach (jak?) przetwarzania danych.

Na przykład:

- pracodawca w stosunku do danych osobowych swoich pracowników – administrator danych,
- sprzedawca w sklepie internetowym w stosunku do danych osobowych swoich klientów – administrator danych,
- właściciel strony internetowej w stosunku do danych osobowych osób, które zaprenumerowały newsletter – administrator danych.

(WAŻNE: Biuro Rachunkowe BATAX jest zatem administratorem danych swoich pracowników i danych swoich Klientów – w zakresie wykonywania umowy o świadczenie usług księgowych, np. wystawienie faktury za usługi księgowe)

Administrator danych to zawsze określony podmiot, a nie jego pracownik.
Na przykład:

- spółka z o.o. – administrator danych,
- prezes zarządu spółka z o.o. – nie jest administratorem danych,
- Jan Kowalski, prowadzący jednoosobową działalność gospodarczą – administrator danych.

✓ **Podmiot przetwarzający dane osobowe** nie decyduje o celach (po co?) i sposobach (jak?) przetwarzania danych; działa natomiast na podstawie umowy z administratorem danych. Administrator danych może bowiem przetwarzać dane samodzielnie albo też może skorzystać z usług zewnętrznego podmiotu, który te dane będzie dla niego przetwarzał (podmiot przetwarzający dane osobowe).

Na przykład:

- biuro rachunkowe jest podmiotem przetwarzającym dane osobowe, ponieważ przetwarza na zlecenie dane osobowe przekazane mu w tym celu przez klientów,
- firma utrzymuje na zlecenie swoich klientów konta poczty elektronicznej – jest podmiotem przetwarzającym dane osobowe, ponieważ przetwarza na zlecenie dane osobowe klientów-zleceniodawców,
- firma zajmuje się profesjonalnie niszczeniem danych osobowych – jest podmiotem przetwarzającym dane osobowe, ponieważ przetwarza w tym zakresie dane osobowe na zlecenie swoich klientów.

(WAŻNE: Biuro Rachunkowe BATAX jest zatem podmiotem przetwarzającym dane swoich Klientów i ich pracowników – zgodnie z zawartą z Klientami umową powierzania przetwarzania danych osobowych, np. w celu prowadzenia usług rachunkowych, usług związanych z ubezpieczeniami społecznymi, itp.)

Każdy podmiot przetwarzający dane na zlecenie powinien zawrzeć z administratorem danych tzw. umowę powierzenia, w której określone zostaną zasady przetwarzania danych.
W firmach dane osobowe faktycznie przetwarzane są przez konkretne osoby fizyczne – pracowników lub współpracowników administratora lub podmiotu przetwarzającego dane. Osoby te powinny posiadać stosowne upoważnienie do takiego przetwarzania danych osobowych.

Podstawa prawna: art. 4 pkt 7 i 8 RODO.

- **Kiedy można przetwarzać dane osobowe:**

Dane osobowe można przetwarzać **wyłącznie wtedy, gdy istnieje do tego podstawa prawna przetwarzania danych.**
W przypadku podmiotów gospodarczych takimi typowymi podstawami przetwarzania danych zwykłych są:

- zgoda osoby, której dane dotyczą, np. wyraźna zgoda osoby, której dane dotyczą
- umowa z osobą, której dane dotyczą, gdy przetwarzanie tych danych jest niezbędne do jej wykonania lub do podjęcia działań poprzedzających zawarcie umowy, na żądanie tej osoby, np.: przetwarzanie danych jest niezbędne do wykonania zadań związanych z zatrudnieniem, ubezpieczeniem społecznym pracowników;
- obowiązek prawny ciążący na administratorze, gdy przetwarzanie jest niezbędne do jego wypełnienia, np.: przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy,
- prawnie uzasadniony interes realizowanych przez administratora lub przez stronę trzecią, gdy przetwarzanie jest niezbędne do osiągnięcia wynikających z niego celów, np.: przetwarzanie danych jest niezbędne w celu dochodzenia praw przed sądem.

Ważne: Administrator danych zawsze powinien móc wykazać, że dysponuje odpowiednią podstawą przetwarzania danych: to obowiązek prawny administratora danych wynikający z tzw. zasady rozliczalności.

Podstawa prawna: art. 6 i 9 RODO.

- **Ile danych można przetwarzać:**

RODO wprowadza tzw. zasadę minimalizacji danych osobowych. Określa ona, **że można przetwarzać wyłącznie takie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania danych.** Dlatego przetwarzanie danych powinno zostać ograniczone tylko do takich danych, bez których nie można osiągnąć celu ich przetwarzania.

Na przykład: firma realizuje zamówienia w sklepie internetowym - firma zawarła jednak w formularzu sklepu pytania o: stan cywilny (sytuacja rodzinna), ilość dzieci w gosp. domowym (sytuacja rodzinna), zarobki (sytuacja finansowa). Firma nie może przetwarzać tych danych w celu realizacji zamówienia: to niedopuszczalne. Mogłaby to robić, ale w innym celu, np.: w celach marketingowych, z tym że na innej podstawie prawnej.

Podstawa prawna: art. 5 ust. 1 pkt c) RODO.

- **Jakie dane przetwarza biuro rachunkowe?**

Dane osobowe przetwarzane w biurze rachunkowym mają źródło w powierzonych przez klientów dokumentach pracowniczych, umowach, fakturach czy wyciągach bankowych. Do kategorii przetwarzanych przez biura rachunkowe danych osobowych i zbiorów danych zawierających informacje gospodarcze w szczególności należą dane o wielkości transakcji klienta, dane jego kontrahentów, dane jego pracowników czy jego samego.

- **Podpisałem umowę powierzenia przetwarzania danych z biurem rachunkowym, kto jest administratorem danych?**

Klient przekazujący dane osobowe (na podstawie umowy powierzenia przetwarzania danych) dla biura rachunkowego **pozostaje administratorem tych danych**. To on jest zobowiązany do zachowania staranności w celu ochrony danych swoich kontrahentów. Nie ma tu znaczenia, że przekazał (powierzył) pieczę nad dokumentami biuru rachunkowemu. Wciąż to klient pozostaje administratorem danych i jest zobowiązany zgodnie z ustawą do dochowania ich należytej ochrony.

Biuro rachunkowe ma za to zadanie dokładać wszelkiej staranności, żeby przetwarzanie danych było zgodne z przepisami prawa.

- **Jak powinna być zgoda na przetwarzanie danych:**

Każda zgoda, dla swej ważności, powinna być:

- dobrowolna – tylko jeżeli osoba, której dane osobowe dotyczą, ma możliwość dokonania rzeczywistego wyboru, a jednocześnie nie zachodzi ryzyko: wprowadzenia w błąd, zastraszenia, przymusu lub znaczących negatywnych konsekwencji, jeśli nie wyrazi zgody. Jeżeli konsekwencje wyrażenia zgody nie dają się pogodzić ze swobodą wyboru, zgoda nie jest wówczas dobrowolna (
- konkretna – musi dokładnie określać cel przetwarzania danych; niedopuszczalna jest zgoda ogólna, która nie określa dokładnego celu przetwarzania
- świadoma – zgodnie z art. 23 ust. 1 pkt 1 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zgoda nie może mieć charakteru abstrakcyjnego, lecz winna odnosić się do skonkretyzowanego stanu faktycznego, obejmując tylko określone dane oraz sprecyzowany sposób i cel ich
- jednoznaczna – musi mieć charakter wyraźny i jasny dla składającego ją w momencie jej wyrażania

- **Forma zgody**

Zgoda na przetwarzanie danych osobowych **może być wyrażona w dowolnej formie** – ważne, by administrator danych w każdej sytuacji, gdy zostaje zgłoszona/wyrażona wątpliwość, mógł wykazać faktyczne jej udzielenie. Administrator danych sam powinien określić i wybrać, w jaki sposób gromadzi i przechowuje zgody na przetwarzanie danych osobowych.

W przypadku zgody na przetwarzanie danych zaliczonych do szczególnych kategorii danych osobowych, RODO – inaczej, niż to ma miejsce na gruncie Ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych – nie wymaga, aby zgoda ta była wyrażona na piśmie. Zgodnie z RODO taka **zgoda powinna być zgodą „wyraźną**"; może więc zostać udzielona np. w Internecie poprzez zaznaczenie odpowiedniego pola wyboru. Oczywiście zbieranie zgód na piśmie w dalszym ciągu będzie dopuszczalne.

Podstawa prawna: art. 6 RODO.

- **Jakie informacje przekazywać przy zbieraniu zgody na przetwarzanie danych osobowych?**

RODO nakazuje, by przy gromadzeniu danych przekazywać osobie, której dane dotyczą, następujące informacje:

- tożsamość administratora danych i o jego dane kontaktowe, a jeżeli administrator danych powołał Inspektora Ochrony Danych (IOD), to dane kontaktowe IOD;
- cel i podstawę przetwarzania danych, a jeżeli przetwarzanie odbywa się na tej podstawie, że jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią – prawnie uzasadniony interes;
- na temat odbiorcy danych osobowych lub kategorii odbiorców, jeżeli istnieją;
- zamiar przekazania danych osobowych do państwa trzeciego w każdym przypadku, gdy ma to zastosowanie;
- czas, przez jaki dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- prawo do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub informacje o prawie do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych;
- prawo do cofnięcia zgody w dowolnym momencie, jeżeli przetwarzanie odbywa się na podstawie zgody;
- prawo wniesienia skargi do organu nadzorczego;
- informacja, 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;
- wiadomość o tzw. zautomatyzowanym podejmowaniu decyzji lub profilowania, w każdym przypadku jeżeli dochodzi do tego dochodzi wraz z zasadami automatycznego podejmowania decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
- wskazanie podmiotów przetwarzających dane osobowe na zlecenie administratora danych.

- **Kiedy nie muszę zbierać zgody na przetwarzanie danych?**

Zgody na przetwarzanie danych nie trzeba zbierać w szczególności wtedy, gdy:

- przetwarzanie danych jest niezbędne do wykonania umowy, np. sklep internetowy sprzedaje wysyłkowo książki - nie musi w takim wypadku prosić o zgodę na przetwarzanie danych, przetwarzanie danych będzie zgodne z RODO jako niezbędne do wykonania umowy (sprzedaży);

- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, np. przetwarzanie danych w celach związanych z prowadzeniem ksiąg rachunkowych nie wymaga zgody osób, których dane dotyczą, a jego podstawą są przepisy o rachunkowości;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, np. skierowanie do sądu pozwu o zapłatę przeciwko nieuczciwemu klientowi nie wymaga jego zgody na przetwarzanie danych, a podstawą przetwarzania danych w takim wypadku jest właśnie realizacja prawnie uzasadnionego interesu administratora danych.

Prawnie uzasadnionym interesem realizowanym przez administratora danych jest także marketing jego produktów i usług. Przetwarzanie danych w takim celu – marketingowym w stosunku do produktów i usług administratora danych – nie wymaga zgody na przetwarzanie danych osobowych.
Ważne: pewne formy kontaktu z osobami, których dane dotyczą**, wymagają zgody**:

- przesyłanie informacji handlowej za pomocą środków komunikacji elektronicznej, np. reklam za pomocą poczty elektronicznej,
- wykorzystanie telekomunikacyjnych urządzeń końcowych w celu marketingu bezpośredniego, np. wysyłanie wiadomości SMS o treści reklamowej.

Podstawa prawna:
art. 6, art. 12 i 13 RODO,
art. 10 Ustawy o świadczeniu usług drogą elektroniczną,
art. 172 ustawy Prawo telekomunikacyjne.

- **Co to jest upoważnienie do przetwarzania danych osobowych?**

Każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.
Na przykład:

- Pracownik biura rachunkowego może przetwarzać dane na podstawie upoważnienia od przedmiotu przetwarzającego,
- Pracownik może wystawiać faktury lub wykonywać zapłatę z firmowego konta bankowego na podstawie upoważnienia administratora

Podstawa prawna:
art. 29 RODO

- **Czy mogę odwołać zgodę na przetwarzanie danych?**

Zawsze można odwołać złożoną zgodę na przetwarzanie danych osobowych.
Ważne: odwołanie zgody powinno być tak samo łatwe, jak jej udzielenie.

Na przykład: złożyłeś swoją zgodę na przetwarzanie danych osobowych podczas wizyty na stronie internetowej; powinieneś mieć możliwość jej odwołana również przez stronę internetową.

Od chwili otrzymania oświadczenia o odwołaniu zgody, nie można już powoływać się na zgodę na przetwarzanie danych osobowych; odwołanie zgody wywołuje wyłącznie skutki na przyszłość. Tym samym – wszystkie wcześniejsze czynności, które opierały się na tej zgodzie, pozostają ważne.

Podstawa prawna: art. 7 ust. 3 RODO.

- **Jak długo można przechowywać dane osobowe?**

Przechowywanie dane osobowych powinno być ograniczone czasowo: nie powinny być przechowywane w nieskończoność.
W przypadku gdy przetwarzanie danych osobowych odbywa się na podstawie:

- zgody, to dane osobowe mogą być przetwarzane tak długo, aż zgoda ta nie zostanie odwołana; po odwołaniu zgody dane mogą być przechowywane nie dłużej niż 10 lat, czyli przez czas odpowiadający okresowi przedawnienia roszczeń, jakie może podnosić administrator danych i jakie mogą być podnoszone wobec administratora danych;
- wykonywania umowy, wówczas dane mogą być przetwarzane tak długo, jak jest to niezbędne do wykonania tej umowy – przez czas odpowiadający okresowi przedawnienia roszczeń, jakie może podnosić administrator danych i jakie mogą być podnoszone wobec administratora danych; w przypadku przedsiębiorców ten okres, co do zasady, wynosi nie więcej niż trzy lata i różni się w zależności od tego, jakiej umowy dotyczyło przetwarzanie danych.

Ważne: Jeżeli istnieją przepisy szczególne określające czas, przez jaki powinny być przechowywane dane osobowe, wówczas takie przepisy mogą wydłużać (lub w konkretnym przypadku skracać) czas przetwarzania danych osobowych.
Na przykład: w przepisach o rachunkowości nakaz przechowywania dowodów księgowych dla umów handlowych, roszczeń dochodzonych w postępowaniu cywilnym lub objętych postępowaniem karnym albo podatkowym wynosi pięć lat, od początku roku następującego po roku obrotowym, w którym operacje, transakcje, postępowanie zostały ostatecznie zakończone, spłacone, rozliczone lub przedawnione.

Podstawa prawna: art. 5 ust. 1 pkt e) RODO.

ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

- **Jak zabezpieczać dane osobowe?**

Ciągle obowiązująca polska UOD wskazuje szereg konkretnych środków zabezpieczenia danych osobowych, jakie mają zostać wdrożone przez administratora lub podmiot przetwarzający. RODO zamiast tego wprowadza tzw. podejście oparte na ryzyku. **Jego istotą jest to, że każdy podmiot przetwarzający dane osobowe powinien samodzielnie określić, jakie konkretne środki zabezpieczenia danych należy wdrożyć.**
Dobór tych środków powinien opierać się o:

- charakter, zakres, kontekst i cele przetwarzania,
- ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia,
- stan wiedzy technicznej,
- koszt wdrażania.

Każdy podmiot przetwarzający dane osobowe powinien więc:

- ustalić, jakie dane osobowe, w jakim charakterze, po co i w jakim środowisku przetwarza,
- kreślić ryzyko naruszenia praw lub wolności osób fizycznych związane z takim przetwarzaniem,
- dobrać odpowiednie środki zabezpieczenia danych, uwzględniając istniejące możliwości techniczne i własne możliwości finansowe.

RODO nie nakazuje stosowania żadnych konkretnych środków zabezpieczenia danych, a jedynie wskazuje przykładowe środki techniczne i organizacyjne, które mogą służyć osiągnięciu tego celu – zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku.
Są to w szczególności:

- pseudonimizacja i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Takie podejście – **oparte na ryzyku –** zakłada, że każdy podmiot przetwarzający dane w sposób świadomy podejmie decyzję co do zastosowanych środków zabezpieczenia.
Ważne: każdy podmiot przetwarzający dane osobowe ponosi odpowiedzialność w przypadku naruszenia bezpieczeństwa danych osobowych.
Podstawa prawna: art. 32 RODO.

- **Czy nadal muszę prowadzić dokumentację ochrony danych osobowych?**

Ustawa z 29 sierpnia 1997 r. nakładała na administratorów danych obowiązek przygotowania i wdrożenia tzw. dokumentacji ochrony danych osobowych, na która składały się:

- polityka bezpieczeństwa danych osobowych,
- instrukcja zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe.

RODO rezygnuje z tego obowiązku na rzecz podejścia opartego na ryzyku. **Niemniej jednak w treści RODO istnieją liczne odwołania do tzw.: polityk ochrony danych stosowanych przez administratora. Dlatego właśnie nic nie stoi na przeszkodzie – wręcz zaleca się dalsze stosowanie dokumentacji ochrony danych osobowych, oczywiście po jej aktualizacji do przepisów RODO – aby wciąż ją prowadzić.**

(WAŻNE: Biuro Rachunkowe BATAX nie prowadzi dokumentacji ochrony danych osobowych dla swoich Klientów)

- **Co to jest i do czego służy rejestr czynności przetwarzania danych?**

Rejestr czynności przetwarzania danych to ważny elementem dokumentacji ochrony danych. Rejestr powinien być prowadzony odrębnie dla każdego procesu przetwarzania danych – i niektóre z tych procesów występujących w typowych organizacjach mogą być zwolnione z prowadzenia rejestru. **Obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych należy do administratora danych oraz podmiotu przetwarzającego dane**.

1. ADO odnotowuje w rejestrze czynności przetwarzania:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów oraz przedstawiciela administratora oraz Inspektora Ochrony Danych (IOD) – gdy ma to zastosowanie,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
- przekazania danych osobowych do państwa trzeciego – gdy ma to zastosowanie,
- planowane terminy usunięcia poszczególnych kategorii danych – jeżeli jest to możliwe,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych – jeżeli jest to możliwe.

2. Podmiot przetwarzający odnotowuje w rejestrze czynności przetwarzania:

- imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający,
- kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
- przekazania danych osobowych do państwa trzeciego – gdy ma to zastosowanie,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych – jeżeli jest to możliwe.

Rejestr może być prowadzony zarówno w formie papierowe, jak i w postaci elektronicznej.
Rejestr czynności nie musi być prowadzony przez przedsiębiorców zatrudniających mniej niż 250 osób, chyba że:

- przetwarzanie może naruszać prawa lub wolności osób, których dane dotyczą,
- przetwarzanie obejmuje szczególne kategorie danych lub dane dotyczące wyroków skazujących,
- przetwarzanie nie ma charakteru sporadycznego.

- **Czy muszę wyznaczyć IOD (Inspektora Ochrony Danych)?**

Inspektor Ochrony Danych (IOD) to następca Administratora Bezpieczeństwa Informacji (ABI). Wyznaczenie IOD wg **RODO jest obowiązkowe, gdy** (inaczej niż teraz w przypadku ABI):

- dane są przetwarzane przez podmioty z sektora publicznego,
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących.

Główna działalności oznacza działalność kluczową z punktu widzenia osiągnięcia celów administratora albo podmiotu przetwarzającego dane. Nie każdy podmiot, którego główną działalnością jest przetwarzanie danych, musi jednak powołać IOD: **tylko taki, którego działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę.**
Działalność główna to także ta, która jest nierozerwalnie związaną z działalnością główną.

- **Czym jest naruszenie ochrony danych (incydent bezpieczeństwa)?**

RODO mianem „incydentu bezpieczeństwa" określa naruszenie bezpieczeństwa prowadzące do:

- przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania danych osobowych,
- nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Na przykład:
Z naruszeniem ochrony danych – incydentem bezpieczeństwa – mamy do czynienia, gdy:

- serwisant zgubi nośnik z danymi osobowymi klientów firmy, w której pracuje;

- magazynier w sklepie internetowym uzyska dostęp do danych osobowych wszystkich klientów firmy kurierskiej poprzez system wysyłki paczek;
- w firmie nastąpiła kradzież danych pracowników poprzez włamanie do systemu kadrowo-płacowego firmy.

Ale naruszeniem ochrony danych osobowych nie będzie błędne czy niepełne wypełnienie obowiązku informacyjnego bądź wadliwie skonstruowanie zgody jako podstawy prawnej przetwarzania danych osobowych.

Podstawa prawna: art. 35 RODO.

- **Kiedy muszę zgłosić naruszenie danych osobowych (incydent bezpieczeństwa)?**

RODO nakłada na administratorów danych osobowych (ADO) szereg nowych praw i obowiązków. **Jednym z nich jest obowiązek zawiadomienia organu nadzorczego o naruszeniu przetwarzania danych osobowych**, zwany obowiązkiem notyfikacji naruszeń.
To bardzo istotna zmiana w stosunku do ustawy o ochronie danych osobowych z 29 sierpnia 1997 r., która tego rodzaju rozwiązania w ogóle nie zawierała.
Norma zawarta w RODO nie nakłada na administratorów danych obowiązku informowania organu nadzorczego o jakimkolwiek incydencie związanym z przetwarzaniem danych osobowych. Obowiązek notyfikacji (zgłoszenia naruszenia) jest związany z takim zdarzeniem, którego efektem jest naruszenie bezpieczeństwa przetwarzanych danych.
Ważne: naruszenie powinno prowadzić do wystąpienia określonego skutku w odniesieniu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, w postaci:

- zniszczenia,
- utracenia,
- zmodyfikowania,
- nieuprawnionego ujawnienia
- nieuprawnionego dostępu.

Nie ma znaczenia, czy naruszenie związane było z działaniem przypadkowym czy niezgodnym z prawem.
O wystąpieniu incydentu bezpieczeństwa należy poinformować organ nadzorczy (PUODO). Informacja powinna zostać przekazania niezwłocznie, lecz nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.

- **Co powinno zawierać zgłoszenie naruszenia danych osobowych (incydent bezpieczeństwa)?**

Zgłoszenie naruszenia do PUODO (po jego powołaniu) powinno zawierać:

- opis charakteru naruszenia, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą,
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych (ABI),
- opis możliwych konsekwencji naruszenia,
- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych oraz minimalizowaniu negatywnych skutków naruszenia.

Ważne: na dzień dzisiejszy nie ma jeszcze ostatecznych przepisów, które w szczegółowy sposób określają formę i tryb mający zastosowanie przy realizacji obowiązku notyfikacji.

- **Czy o naruszeniu danych osobowych (incydent bezpieczeństwa) muszę informować osoby, których te dane dotyczą?**

Tak, gdy naruszenie – incydent – może powodować wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą.
Na przykład o naruszeniu danych osobowych musisz poinformować osoby, których to naruszenie dotyczy, gdy:

- nieuprawniony pracownik banku uzyska dostęp do loginów i haseł wszystkich klientów systemu bankowości elektronicznej,
- gdy serwisant firmy informatycznej zgubi pendrive zawierający dokumentację medyczną pacjentów szpitala, którego sprzęt serwisuje.

Nie, gdy, w szczególności:

- zostały wdrożone odpowiednie środki ochrony,
- środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie (w szczególności środki takie, jak szyfrowanie danych).

Ważne: zgodnie z propozycją Ministerstwa Cyfryzacji obowiązki związane ze zgłaszaniem incydentów mają zostać wyłączone w stosunku do przedsiębiorców zatrudniających mniej niż 250 osób, przetwarzających dane osobowe niezbędne do wykonywania działalności gospodarczej, w szczególności w celu zawierania umów i prowadzenia rachunkowości.

Podstawa prawna: art. 33 i 4 RODO.

- **Co to jest: powierzenie przetwarzania danych?**

W stosunku do ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych RODO bardzo szczegółowo, nawet drobiazgowo, reguluje instytucję powierzenia przetwarzania danych osobowych, pozycję procesora oraz relacje między tymi podmiotami.
Administrator Danych Osobowych nie musi bowiem sam przetwarzać danych osobowych – może je przekazać do przetwarzania innemu podmiotowi: procesorowi. W działalności większości przedsiębiorców dochodzi do powierzenia przetwarzania danych osobowych.
Podmiotem, któremu ADO może powierzyć przetwarzanie danych osobowych może być zarówno osoba fizyczna jak i prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
Na przykład:

- firma przekazuje prowadzenie ksiąg rachunkowych do biura rachunkowego,
- firma korzysta z usług operatora zapewniającego usługi poczty elektronicznej,
- podczas przeprowadzki firma zleca specjalistycznej firmie zniszczenie dokumentów zawierających dane osobowe,
- firma zleca specjalistycznej firmie archiwizację dokumentów zawierających dane osobowe.

Jeżeli administrator (ADO) chce powierzyć przetwarzanie danych w jego imieniu, to może w tym celu 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.
RODO nakazuje ADO dołożenie szczególnej staranności przy wyborze procesora.
Na administratorze ciąży prawna i biznesowa odpowiedzialność za przetwarzane dane.
Podmiot przetwarzający dane na zlecenie powinien zawrzeć z administratorem danych odpowiednią umowę, tzw. umowę powierzenia, w której określone zostaną zasady przetwarzania danych.

Podstawa prawna: art. 28 RODO.

- **Co oznacza „prawo do bycia zapomnianym”?**

RODO daje każdemu, kogo dotyczą dane, nowe uprawnienie w postaci prawa do bycia zapomnianym (prawo do usunięcia danych). To faktycznie dwa uprawnienia:

- możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez administratora danych,
- możliwości żądania, aby administrator danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych lub ich kopie.

Prawo do bycia zapomnianym można wykonać, jeżeli spełniona jest choćby jedna z poniższych przesłanek:
dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

- osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych;
- osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją:
- szczególną sytuacją,
- albo sprzeciw wobec przetwarzania danych dla celów marketingowych,
- dane osobowe były przetwarzane „niezgodnie z prawem”;
- dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator”;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

Na przykład:
Firma handlowa przetwarza moje dane osobowe na podstawie złożonej przez mnie zgody na przetwarzanie danych w celu marketingowym. Wycofuję moją zgodę i korzystam z prawa do bycia zapomnianym. Firma (ADO) powinna zaprzestać przetwarzania moich danych osobowych i usunąć je, chyba że zachodzą szczególne przypadki ograniczające moje prawo do bycia zapomnianym.
Do obowiązków ADO w zakresie wykonania prawa do bycia zapomnianym należy również wspomniane wyżej poinformowanie innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

Ale: obowiązek ten nie ma charakteru nieograniczonego i może być ograniczony przez:

- dostępną technologię,
- koszty,
- konieczność ograniczenia do „rozsądnych działań".

A więc będziemy mieli do czynienia z sytuacjami, w których podmioty większe, o większych możliwościach technologicznych oraz finansowych będą zobowiązane do wykonywania tego obowiązku w szerszym zakresie niż podmioty niewielkie, mające mniejsze dostępne zasoby technologiczne i finansowe. Natomiast ograniczenie do rozsądnych działań oznacza, że obowiązek nie ma charakteru zobowiązania co do rezultatu, a wyłącznie starannego działania.

Podstawa prawna: art. 17 RODO.

- **Czy zawsze można skorzystać z prawa do bycia zapomnianym?**

Nie, prawo do bycia zapomnianym nie ma zastosowania jeśli przetwarzanie jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- z uwagi na:
  - cele zdrowotne,
  - interes publiczny w dziedzinie zdrowia publicznego;
  - do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
  - do ustalenia, dochodzenia lub obrony roszczeń.

Na przykład:

- zamówiłeś książkę w sklepie internetowym – otrzymałeś ją, ale jeszcze za nią nie zapłaciłeś; składasz wniosek o realizację prawa do bycia zapomnianym; ADO-sklep internetowy może Twoje dane nadal przetwarzać, ponieważ są niezbędne do dochodzenia roszczeń sklepu, do czasu zapłaty lub dochodzenia praw przed sądem;
- zamówiłeś książkę w sklepie internetowym – zapłaciłeś za nią i otrzymałeś ją; składasz wniosek o realizację prawa do bycia zapomnianym; ADO-sklep internetowy może Twoje dane nadal przetwarzać, ponieważ obowiązek przetwarzania danych wynika z przepisów o rachunkowości.

Podstawa prawna: art. 17 RODO.

- **Co to jest prawo do przenoszenia danych?**

To prawo do:

- otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych, które dostarczyła administratorowi,
- przesłania przez osobę, której dane dotyczą, danych osobowych, które dostarczyła administratorowi, innemu administratorowi, bez przeszkód ze strony administratora danych.

Prawo to może być wykonane wyłącznie wtedy, gdy przetwarzanie danych odbywa się:

- na podstawie zgody lub w celu wykonania umowy,
- w sposób zautomatyzowany.

Prawo do przenoszenia danych obejmuje tylko dane osobowe przetwarzane przy użyciu systemów informatycznych i nie obejmuje tradycyjnych, papierowych zbiorów danych.
Format danych nadający się do odczytu maszynowego to format pliku zorganizowany tak, aby aplikacje komputerowe mogły łatwo zidentyfikować, rozpoznać i uzyskać określone dane, np.: pliki w formacie XML, JSON, CSV.
Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo i które to dane ta osoba dostarczyła administratorowi. W pewnych przypadkach dane objęte prawem do przeniesienia będą jednak obejmować także dane innych osób.

Na przykład:

- postanawiasz zmienić bank. Dotychczasowy bank powinien zapewnić Ci możliwość przeniesienia twoich danych do nowego banku;
- rezygnujesz z abonamentu do słuchania muzyki przez Internet i wybierasz nowy serwis; dotychczasowy dostawca powinien umożliwić Ci przeniesienie danych, w tym np.: twoich play list do nowego dostawcy.

Podstawa prawna: art. 20 RODO.

➢ **Kiedy nie mogę skorzystać z prawa do przeniesienia danych?**

Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego:

- w interesie publicznym,
- w ramach sprawowania władzy publicznej powierzonej administratorowi.

Prawa tego – z uwagi na jego charakter – nie powinno się wykonywać w stosunku do administratorów przetwarzających dane osobowe w ramach wykonywania obowiązków publicznych. Dlatego nie powinno ono mieć zastosowania w przypadkach, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

➢ **Czy mogę skorzystać jednocześnie z prawa do przeniesienia danych i do zapomnienia?**

Osoba, której dane dotyczą, ma prawo żądania od administratora (ADO) niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
Osoba, której dane dotyczą (z uwzględnieniem celów przetwarzania), ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Podstawa prawna: art. 16 RODO.

RODO A PRACOWNICY

➢ **Jakich danych można będzie żądać od kandydata i od pracownika?**

- Dane od kandydata do pracy:

Obecnie pracodawca ma prawo żądać od kandydata na pracownika podania: imienia i nazwiska, imion rodziców, daty i miejsce urodzenia, adresu do korespondencji, wykształcenia oraz przebiegu dotychczasowego zatrudnienia.

Po wejściu w życie nowych przepisów pracodawca nie będzie już mógł żądać od osoby ubiegającej się o zatrudnienie podania imion rodziców oraz adresu zamieszkania. Zamiast adresu zamieszkania pracodawca będzie jednak mógł uzyskać adres do korespondencji oraz adres poczty elektronicznej albo numer telefonu kandydata.

- Dane od pracownika:

Jeżeli kandydat zostanie zatrudniony, pracodawca będzie mógł żądać od niego podania adresu zamieszkania, imion rodziców. Ponadto od pracownika (ale nie kandydata) można obecnie żądać podania numeru PESEL oraz innych danych osobowych pracownika, a także danych osobowych dzieci pracownika i innych osób z jego najbliższej rodziny, jeżeli jest to konieczne dla realizacji szczególnych uprawnień pracownika wynikających z przepisów prawa pracy i ubezpieczeń społecznych – np. zgłoszenie do ZUS.

➢ **Czy w wystarczającym jest umieszczenie w aktach osobowych pracownika klauzuli informacyjnej wynikającej z ustawy RODO? Czy też każdy pracownik musi ją wpierw podpisać?**

RODO nie wymaga aby obowiązek informacyjny spełniony był tylko i wyłącznie w formie pisemnej z dodatkowym podpisem pracownika, który potwierdzi fakt zapoznania się z tą informacją. Jest to jednak sposób rekomendowany, aby móc udowodnić, że obowiązek informacyjny nałożony na szkołę został spełniony. Samo umieszczenie klauzuli w teczce osobowej nie potwierdza, że z tymi informacji zapoznał się pracownik

➢ **Przetwarzanie danych pracownika przez pracodawcę**

Po nawiązaniu stosunku pracy, przetwarzanie adresu do korespondencji oraz adresu poczty elektronicznej lub numeru telefonu pracownika przez pracodawcę będzie możliwe **wyłącznie po wyrażeniu przez niego zgody** w postaci wyraźnego oświadczenia złożonego w formie papierowej lub elektronicznej.
Przetwarzanie danych osobowych kandydata lub pracownika będzie m**ożliwe tylko w zakresie niezbędnym do realizacji stosunku pracy. Zasada ta odnosi się do wszystkich danych osobowych kandydata i pracownika**

- **Przetwarzanie danych biometrycznych pracownika**

Zgodnie z RODO danymi biometrycznym są dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy czy dane daktyloskopijne. Za dane biometryczne uznać należy zdjęcia zamieszczane w CV kandydatów do pracy, czy umieszczane w dyplomach studiów wyższych, których kserokopie często przechowywane są w aktach pracowniczych.

Pracodawca będzie miał prawo przetwarzać wyłącznie te dane biometryczne, które dotyczą stosunku pracy, pod warunkiem uzyskania od pracownika zgody udzielonej w formie papierowej i elektronicznej. Ewentualny brak takiej zgody nie będzie mógł być podstawą do niekorzystnego traktowania kandydata lub pracownika i nie będzie mógł powodować dla nich żadnych negatywnych konsekwencji. W szczególności brak zgody na przetwarzanie danych biometrycznych nie będzie mógł uzasadniać odmowy zatrudnienia, wypowiedzenia stosunku pracy lub jego rozwiązania bez wypowiedzenia przez pracodawcę.

- **Dane objęte zakazem przetwarzania**

RODO wprowadza zakaz przetwarzania danych osobowych obejmujących informacje o nałogach, stanie zdrowia oraz życiu seksualnym i orientacji seksualnej.

Pracodawca nadal będzie mógł zażądać od kandydata i pracownika przedstawienia np. zaświadczenia lekarskiego czy orzeczenia o zdolności do pracy, jeżeli pracownik będzie chciał skorzystać z przysługujących mu w związku z tym uprawnień.

- **Monitoring w miejscu pracy**

Dopuszczalne będzie stosowanie szczególnego nadzoru nad miejscem pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring). Celem wprowadzenia monitoringu będzie mogło być natomiast wyłącznie:

- zapewnienie bezpieczeństwa pracowników,
- ochrona mienia lub zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

Monitoring nie będzie mógł jednak stanowić środka kontroli wykonywania pracy przez pracownika, nie będzie mógł również obejmować pomieszczeń, które nie są przeznaczone do wykonywania pracy, np. łazienek, szatni, stołówek itp.

W opisanych powyżej sytuacjach, w których pracodawca będzie miał prawo stosować monitoring, będzie on zwolniony z obowiązku uzyskania zgody od pracowników. Na pracodawcy spoczywać będzie za to obowiązek poinformowania pracowników o prowadzonym monitoringu – dotychczasowi pracownicy będą informowani o wprowadzeniu monitoringu nie później niż 14 dni przed jego uruchomieniem, zaś nowi – przed dopuszczeniem ich do pracy.

- **Kto jest administratorem danych osobowych pracowników?**

Administratorem danych pracowników jest zawsze pracodawca – nawet po powierzeniu przetwarzania danych osobowych pracowników innemu podmiotowi.
Przykłady:
Powierzenia obsługi BHP zakładu pracy firmie specjalistycznej – administratorem danych pracowników jest pracodawca,
Powierzenie obsługi kadrowej płacowej biuru rachunkowemu – administratorem danych jest pracodawca,
Skierowanie pracownika na szkolenie – administratorem danych jest pracodawca

- **Co z kserowaniem dowodów/praw jazdy/aktów zgonu/aktów urodzenia/aktów zawarcia związku małżeńskiego?**

Pracownik ma prawo do tzw. „urlopu okolicznościowego”. Potrzeba spędzenia dnia poza pracą jest często związana z istotnymi sytuacjami życiowymi pracownika np. zawarcie związku małżeńskiego, urodzenie dziecka czy śmierć członka jego rodziny. W wielu przypadkach pracodawca żąda w tym wypadku przesłania kserokopii aktu zawarcia związku małżeńskiego czy aktu urodzenia dziecka. Taka praktyka jest niedopuszczalna, ponieważ zebrane w ten sposób dane (np. dane dotyczące dziecka

pracownika) nie są adekwatne do celu ich przetwarzania, czyli stwierdzenia czy pracownikowi przysługuje urlop. W takich sytuacjach dobrą praktyką jest odebranie od pracownika pisemnego oświadczenia potwierdzającego dane wydarzenie.

Ważne: Dobrą praktyką jest pobieranie od pracowników pisemnych oświadczeń - czy to dotyczących aktów urodzenia, zgonu - urlop okolicznościowy, czy posiadanego prawa jazdy. Unikamy wtedy przetwarzania danych osobowych niewspółmiernych do celu jaki nam przyświeca.

Podobna sytuacja tyczy się kserowania prawa jazdy przez pracodawcę w celu uzyskania potwierdzenia posiadania przez pracownika odpowiednich uprawnień dotyczących kierowania samochodem. **W takiej sytuacji pracodawca może zażądać okazania przez pracownika aktualnego prawa jazdy i podpisania stosownego oświadczenia.**

- **Udostępnianie danych pracowników innym organom (policja, prokuratura, komornicy)**

Komornicy, prokuratorzy czy policjanci są pracownikami organów państwowych. W związku z powyższym **pracodawca nie musi uzyskać zgody od pracownika**, aby udostępnić powyższym podmiotom dane osobowe, nie musi też informować pracownika o tym fakcie. Pracownicy organów państwowych w ramach swojej działalności nie muszą też informować osoby, której dane dotyczą o ich przetwarzaniu, gdyż nie stanowią oni tzw. kategorii odbiorców danych. Warto zauważyć, że powyższe rozwiązanie tyczyć będzie się też kuratorów sądowych i społecznych, którzy zbierają dane osobowe w celu realizacji swoich obowiązków zawodowych.