A. Dane osobowe

Oznaczają 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 (art. 4 pkt 1).

Jeśli dane nie stwarzają możliwości zidentyfikowania konkretnej osoby, to nie są to dane osobowe. Dane osobowe dotyczą tylko osób fizycznych, a nie osób prawnych.

Szczególne kategorie danych osobowych (art. 9): dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne (przetwarzane w celu zidentyfikowania osoby fizycznej), dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

B. Wybrane zasady dotyczące przetwarzania danych (art. 5)

- ➔ Ustalamy cele przetwarzania danych.
- ➔ Przetwarzamy tylko zgodnie z ustalonymi celami.
- ➔ Usuwamy dane niezgodne z celami przetwarzania.
- ➔ Usuwany dane jeśli minął okres uzasadniający przechowywanie danych.
- ➔ Chronimy dane (dostęp osób trzecich, utrata, przetwarzanie niezgodne z celami) wykorzystując środki techniczne i organizacyjne.
- ➔ Potrafimy wykazać przestrzeganie zasad dotyczących przetwarzania danych.

C. Zgodność z prawem przetwarzania danych (art. 6)

Dane mogą być przetwarzane tylko i wyłącznie, gdy można je przypisać do jednego z niżej wskazanych celów.

1. Przetwarzanie za zgodą osoby, której dane dotyczą + wskazaniu celów przetwarzania.
2. Przetwarzanie jest niezbędne dla zawarcia lub wykonania umowy, której stroną jest osoba, której dane dotyczą.
3. Przetwarzanie jest niezbędne dla realizacji przez administratora danych osobowych (dalej: ADO) obowiązku prawnego.
4. Ochrona żywotnych interesów osoby, której dane dotyczą lub ochrony żywotnych interesów innej osoby.

5. Realizacja celów wynikających z prawnie uzasadnionych interesów ADO lub strony trzeciej.
6. Zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO (np. organy samorządu zawodowego).

D. Zgoda na przetwarzanie danych (art. 7)

1. Musimy umieć wykazać, że zgodę wyrażono.
2. Zapytanie o zgodę na przetwarzanie danych musi być wyodrębnione od innych kwestii i innego rodzaju zgód.
3. Zgoda może być w każdej chwili wycofana. Musi to być równie łatwe jak udzielenie zgody.
4. Od wyrażenia zgody na przetwarzanie konkretnych danych (innych niż niezbędne dla zawarcia umowy) nie można uzależniać zawarcia umowy.
5. Obowiązki informacyjne ADO spełnia zanim osoba wyrazi zgodę na przetwarzanie danych.

E. Obowiązek informacyjny

1. Realizowany przez ADO przy pozyskiwaniu danych osobowych.
2. Przekazujemy (art. 13):
   a. dane ADO,
   b. cele przetwarzania danych wraz z podstawą prawną,
   c. informacje o odbiorcach danych (lub kategoriach odbiorców),
   d. informacje o zamiarze przekazania danych do państwa trzeciego,
   e. okres przechowywania danych,
   f. informacje o wszelkich uprawnieniach osoby, której dane dotyczą (żądanie sprostowania, usunięcia, ograniczenia przetwarzania, prawie do wniesienia sprzeciwu, prawie do przenoszenia danych, prawie do cofnięcia zgody na przetwarzanie, prawie do wniesienia skargi do organu nadzorczego),
   g. wskazanie, czy podanie danych jest obowiązkiem ustawowym lub umownym (wykonanie lub zawarcie umowy),
   h. wskazanie czy osoba jest zobowiązana do podania danych oraz jakie są konsekwencje ich niepodania,
   i. informację o prawie do wniesienia sprzeciwu wobec przetwarzania danych (art. 21).
3. Jeśli stwarzamy nowy cel na potrzeby już posiadanych danych, musimy ponowić obowiązek przekazania ww. informacji.
4. Obowiązek informacyjny istnieje również w stosunku do osoby, której dane pozyskaliśmy od innej osoby. Wtedy podajemy poza ww. informacjami, źródło z którego dane pochodzą (art. 14).
5. Obowiązku informacyjnego nie trzeba realizować jeśli jest to niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.

F. Uprawnienia osoby, której dane dotyczą

1. ADO musi respektować takie uprawnienia i umożliwiać ich realizację.
2. Prawo do ustalenia, czy dane osoby zwracającej się z zapytaniem są przetwarzane.

3. Jeśli dane są przetwarzane osoba ta ma prawo uzyskać wszystkie informacje wynikające z obowiązku informacyjnego, o którym mowa w art. 13 i 14.
4. Prawo do bezpłatnego uzyskania kopii danych (art. 15).
5. Prawo do sprostowania danych (art. 16).
6. Prawo do bycia zapomnianym (art. 17) oraz prawo do ograniczenia przetwarzania (art. 18). Nie ma zastosowania m.in., gdy dane są niezbędne do ustalenia, dochodzenia lub obrony roszczeń.
7. Obowiązek informowania każdego odbiorcy danych osobowych o ich sprostowaniu, usunięciu lub ograniczeniu przetwarzania (art. 19). Osoba, której dane dotyczą może zażądać otrzymania informacji o tych odbiorcach.
8. Prawo do przenoszenia danych, jeżeli są przetwarzane w sposób zautomatyzowany. Administrator ma przesłać te dane w formie elektronicznej innemu podmiotowi wskazanemu przez osobę, której dane dotyczą (art. 20).
9. Prawo do sprzeciwu wobec przetwarzania danych (art. 21).
10. ADO realizuje żądanie osoby uprawnionej bez zbędnej zwłoki, czyli tak szybko jak to możliwe. Co do zasady, przy trudniejszych sprawach, graniczny termin to miesiąc od otrzymania żądania (art. 12 ust. 3).
11. Jeśli ADO nie podejmie działań, to niezwłocznie, najpóźniej w terminie miesiąca od otrzymania żądania, informuje o powodzie niepodjęcia działań i poucza o prawie wniesienia skargi do organu nadzorczego i prawie do wniesienia pozwu do sądu powszechnego.
12. ADO może pobrać opłatę za ww. działania lub odmówić podjęcia działań, jedynie gdy żądania są ewidentnie nieuzasadnione lub nadmierne (np. ze względu na ich ustawiczny charakter).

G. Prawo do sprzeciwu (art. 21)

1. W sytuacji przetwarzania danych na potrzeby marketingu bezpośredniego.
2. W sytuacji przetwarzania danych w celach, o których mowa w pkt. C. 5. i 6. opracowania, a równocześnie istnieją przyczyny związane ze szczególną sytuacją osoby wnoszącej sprzeciw.
3. Po otrzymaniu sprzeciwu, o którym mowa w pkt. 1 nie można już przetwarzać danych w celu marketingu bezpośredniego.

H. Obowiązek wdrożenia przez ADO środków technicznych i organizacyjnych służących przetwarzaniu danych zgodnie z prawem (art. 24)

1. RODO nie podaje tych środków. Trzeba jednak umieć wykazać ich wdrożenie.
2. Jedynie w sytuacji, gdy jest to „proporcjonalne w stosunku do czynności przetwarzania”, środki te muszą obejmować co najmniej wdrożenie polityk ochrony danych.

I. Konieczność zawarcia umowy powierzenia (art. 28)

Podmiot przetwarzający (dalej: PP): oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt. 7).

1. Z PP zawieramy umowę zawierającą wymogi z art. 28 ust. 3.

2. Z pracownikiem / stażystą itp. nie zawieramy umowy powierzenia, a jedynie sporządzamy upoważnienie do przetwarzania danych.
3. PP za zgodą ADO może korzystać z innych PP.

J. Rejestr czynności przetwarzania

Należy go prowadzić m.in., gdy przetwarzanie danych nie ma charakteru sporadycznego (art. 30 ust. 5).
Należy go prowadzić w formie papierowej i elektronicznej (art. 30 ust. 3).
PUODO może zażądać udostępnienia rejestru (art. 30 ust. 4).

Rejestr zawiera (art. 30 ust. 1):

1. dane ADO,
2. cele przetwarzania,
3. kategorie osób, których dane dotyczą,
4. kategorie danych osobowych,
5. kategorie odbiorców danych,
6. terminy usunięcia poszczególnych kategorii danych,
7. opis technicznych i organizacyjnych środków bezpieczeństwa z art. 32.

K. Rejestr kategorii czynności przetwarzania

Prowadzi go podmiot przetwarzający dane, czyli ten z którym ADO zawarł umowę powierzenia.
Należy go prowadzić w formie papierowej i elektronicznej (art. 30 ust. 3).
PUODO może zażądać udostępnienia rejestru (art. 30 ust. 4).

Zawiera (art. 30 ust. 2):

1. dane PP,
2. dane administratorów (imię, nazwisko, nazwa, kontakt), którzy powierzyli dane,
3. kategorie przetwarzań dokonywanych w imieniu ADO,
4. opis technicznych i organizacyjnych środków bezpieczeństwa z art. 32.

L. Środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzania (art. 32)

1. Zapewniamy stopień bezpieczeństwa odpowiadający ryzyku. Katalog otwarty środków.
2. Szyfrowanie danych.
3. Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.
4. Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

5. Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
6. ADO podejmuje działania, żeby każda osoba mająca dostęp do danych przetwarzała je wyłącznie na polecenie ADO.

M. Środki ochrony prawnej

1. Wniesienie skargi do PUODO (art. 77 ust. 1): jeżeli przetwarzanie danych osobowych narusza rozporządzenie. Uprawnienie do wniesienia skargi dla osoby, której dane dotyczą.
2. Wniesienie pozwu do sądu przeciwko ADO (art. 79).
3. Kary pieniężne wynoszą do 20.000.000 EUR lub do 4 % rocznego światowego obrotu z poprzedniego roku obrotowego (art. 83).

N. Polska ustawa o ochronie danych osobowych

1. Próba obstrukcji postępowania administracyjnego (np. niewydanie dokumentów, nieudzielenie wyjaśnień, niestawienie się przed organem): 500 – 5000 zł grzywny za każde naruszenie (art. 69 uodo).
2. Kontrola możliwa z urzędu lub na wniosek (art. 78 udodo).
3. Możliwość kontroli bez udziału przedsiębiorcy (art. 83 uodo).
4. Kontrolujący ma prawo do wstępu w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń, wglądu do dokumentów, oględzin urządzeń, żądanie pisemnych lub ustnych wyjaśnień, przesłuchiwania osób, uzyskania pomocy Policji w razie problemów w trakcie kontroli.
5. Do protokołu z kontroli można wnieść zastrzeżenia w terminie 7 dni.
6. Kontrola trwa do 30 dni.
7. Grzywna, kara ograniczenia wolności lub pozbawienia wolności do lat dwóch za utrudnianie lub udaremnianie kontroli (art. 108 udodo).
8. Identyczna kara za przetwarzanie danych osobowych choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest się uprawnionym.

O. Co należy zrobić w związku z powyższymi przepisami? Lista obowiązków.

1. Ustalenie jakie dane są przetwarzane. Należy ustalić co jest danymi osobowymi w ramach prowadzonej działalności i jakie czynności stanowią ich przetwarzanie, zgodnie z art. 4 pkt 1) i 2) RODO.
2. Pogrupowanie danych na poszczególne kategorie i przyporządkowanie ich do konkretnych celów przetwarzania danych, zgodnie z art. 5 ust. 1 lit. b) i art. 6 RODO.
3. Ustalenie jakie dane należy usunąć, w związku z brakiem celów ich przetwarzania, zgodnie z art. 5 ust. 1 lit. d) RODO.
4. Ustalenie nowych celów przetwarzania danych, w przypadku chęci gromadzenia konkretnych kategorii danych.
5. Ustalenie okresu w jakim możliwe jest przetwarzanie danych i czasu po jakim konieczne jest ich usunięcie, zgodnie z art. 5 ust. 1 lit. e) RODO.

6. Ustalenie, czy przetwarzanie dotyczy tzw. szczególnych kategorii danych osobowych, co wiąże się z koniecznością wprowadzenia dodatkowych procedur, zgodnie z art. 9 RODO.
7. Przygotowanie procedur i dokumentów zapewniających przetwarzanie danych w myśl zasady integralności i poufności. Konieczne jest istnienie procedur zapewniających ochronę danych przed niezgodnym z prawem lub ustalonymi celami przetwarzaniem, utratą, zniszczeniem lub uszkodzeniem danych, zgodnie z art. 5 ust. 1 pkt f) RODO. Wdrożenie takich procedur i dokumentów może nastąpić w formie tzw. Polityki ochrony danych, o której mowa w art. 24 ust. 2 RODO.
8. Weryfikacja treści umów zawieranych pomiędzy administratorem a klientem końcowym, w celu wykazania, że konkretne kategorie danych są bezpośrednio związane z koniecznością realizacji umowy, zgodnie z art. 6 ust. 1 lit. b) RODO. W zakres weryfikacji wchodzi ewentualna modyfikacja treści takich umów, w celu prostszego wykazania, że dane kategorie danych są niezbędne dla wykonania umowy.
9. Przygotowanie dokumentu / procedury potwierdzającej wyrażenie zgody na przetwarzanie danych, jeśli zgoda taka jest wymagana, zgodnie z art. 7 RODO.
10. Przygotowanie procedury usuwania danych osobowych w taki sposób, aby możliwe było wykorzystywanie pozostałych danych, które kiedyś dotyczyły danej osoby, zgodnie z art. 11 RODO.
11. Przygotowanie dokumentu z informacjami wymaganymi przez RODO, dla osoby, której dane są przetwarzane, a także przygotowanie procedur sprostowania, usuwania, ograniczenia przetwarzania i przenoszenia danych, zgodnie z art. 12 - 20 RODO.
12. Przygotowanie wzoru dokumentu / informacji o prawie do wniesienia sprzeciwu przy przetwarzaniu danych na potrzeby marketingu, zgodnie z art. 21 ust. 3 i 4 RODO.
13. Przygotowanie umowy powierzenia, którą należy zawrzeć z podmiotem, który ma dostęp do jakichkolwiek gromadzonych przez nas danych (np. wystawiane faktury), zgodnie z art. 28 RODO.
14. Przygotowanie upoważnień dla pracowników, stażystów itp. do przetwarzania danych osobowych, z uwzględnieniem konkretnych kategorii danych, zgodnie z art. 37 i 39 Ustawy o ochronie danych osobowych.
15. Przygotowanie rejestru czynności przetwarzania danych osobowych, w sytuacji gdy przetwarzanie danych nie ma charakteru sporadycznego lub ma zastosowanie inna przesłanka, zgodnie z art. 30 ust. 5 RODO.
16. Przygotowanie rejestru kategorii czynności przetwarzania, jeśli jesteśmy podmiotem, któremu powierzono przetwarzanie danych, zgodnie z art. 30 ust. 2 RODO.
17. Przeszkolenie osób, które przetwarzają dane osobowe, ze szczególnym uwzględnieniem uprawnień osób, których dane osobowe są przetwarzane oraz ze szczególnym uwzględnieniem uprawnień organów kontrolnych.