
lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

GDPR RISK TRACKER

by lubasz&wspólnicy

Dokumentacja ochrony danych osobowych zgodnie z zasadą rozliczalności

Wojciech Grenda

dr Dominik Lubasz

lubasz&wspólnicy

KANCELARIA RADCÓW PRAWNYCH

Prelegent

Dominik Lubasz – doktor nauk prawnych, radca prawny, partner zarządzający w Lubasz i Wspólnicy – Kancelaria Radców Prawnych

Ekspert Stowarzyszenia Konsumentów Polskich ds. handlu elektronicznego, a także ekspert legislacyjny Izby Gospodarki Elektronicznej Ecommerce Polska.

W roku 2017 i 2018 otrzymał rekomendację GLOBAL LAW EXPERTS w zakresie prawa ochrony danych osobowych, zaś w roku 2018, 2019 i 2020 rekomendację CHAMBERS AND PARNTER oraz w roku 2020 rekomendację LEGAL 500 również w zakresie prawa ochrony danych osobowych.

Jest członkiem rady naukowej Centrum Ochrony Danych i Zarządzania Informacją Uniwersytetu Łódzkiego, członkiem rady naukowej SABI Stowarzyszenia Inspelktorów Ochrony Danych, członkiem rady naukowej Instytutu Compliance, członkiem komisji rewizyjnej Stowarzyszenia Prawa Nowoczesnych Technologii.

Jest współtwórcą aplikacji do analizy ryzyka wymaganej przepisami RODO – GDPR Risk Tracker.

Prelegent

Wojciech Grenda – absolwent Politechniki Łódzkiej na Wydziale Informatyki, specjalizacja „Sztuczna inteligencja i inżynieria oprogramowania”.

Zawodowo od lat zaangażowany w projektowanie, tworzenie i wdrażanie systemów informatycznych. Zrealizował projekty międzynarodowe oraz ogólnokrajowe, a także dziesiątki mniejszych przedsięwzięć.

Posiadający także wieloletnie doświadczenie w zakresie technicznych i informatycznych aspektów przetwarzania danych oraz bezpieczeństwa informacji.

Prezes zarządu i współtwórca GDPR Risk Tracker, aplikacji i metody analizy ryzyka wymaganej przepisami RODO.

GDPR RISK TRACKER
by lubasz&wspólnicy

Technologiczna neutralność

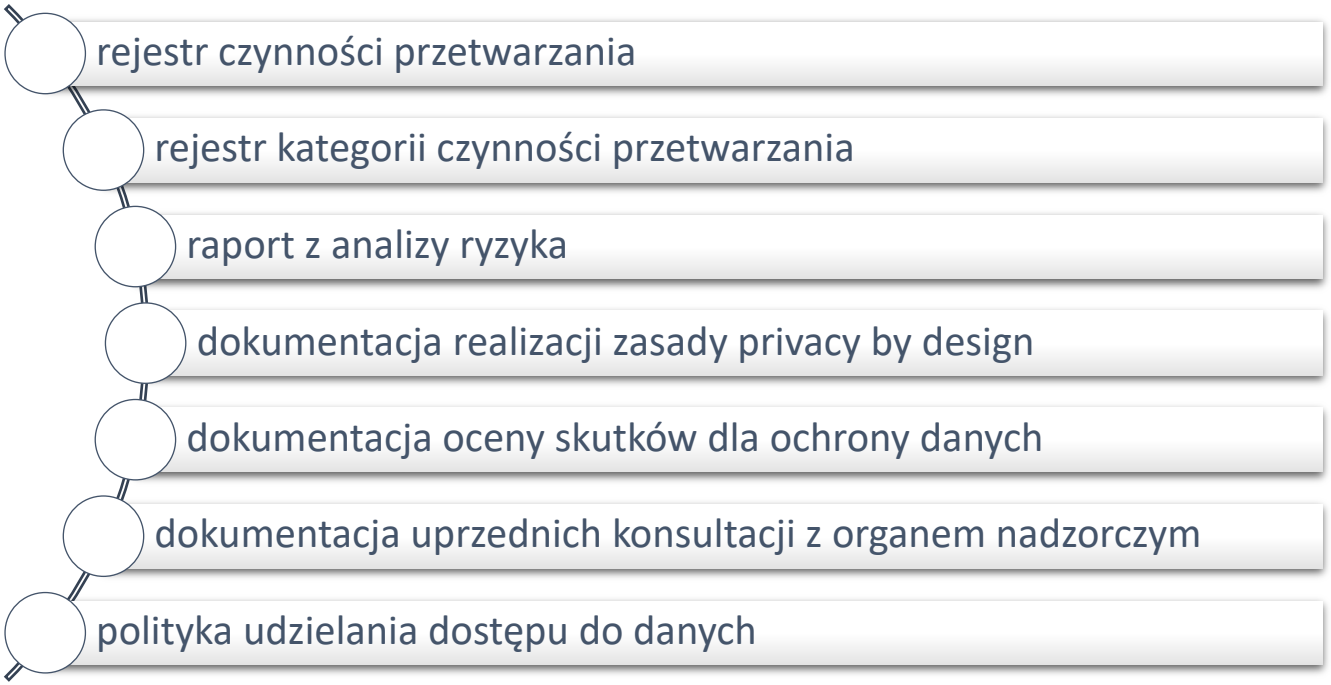
Podejście oparte na ryzyku – ujęcie holistyczne

Adekwatność

Uwzględnienie wpływu przetwarzania na prawa i wolności osoby, której dane dotyczą

Rozliczalność – Domniemanie winy?

Dokumentacja = Rozliczalność?



Dokumentacja = Rozliczalność?

- dokumentacja wszelkich naruszeń ochrony danych osobowych
- dokumentacja powierzeń i poleceń przekazanych procesorom
- dokumentacja spełnienia przesłanek legalizacyjnych
- dokumentacja przekazywania danych do państw trzecich
- polityka retencji danych
- dokumentacja realizacji praw podmiotów danych
- polityka ochrony danych

GDPR RISK TRACKER
by lubasz&wspólnicy

Zgodności z zasadami

Podstawy przetwarzania

Powierzenia przetwarzania

Transfery do państw trzecich

Prawa podmiotów danych

Obowiązki oparte na ryzyku

GDPR RISK TRACKER
by lubasz&wspólnicy

Ogólny obowiązek zapewnienia zgodności

Privacy by design

Privacy by default

Bezpieczeństwo przetwarzania

Ocena skutków dla ochrony danych

Data protection impact assessment

Zgłoszenie naruszenia

Dokumentacja

GDPR
RISK TRACKER
by lubasz&wspólnicy

KONTEKST

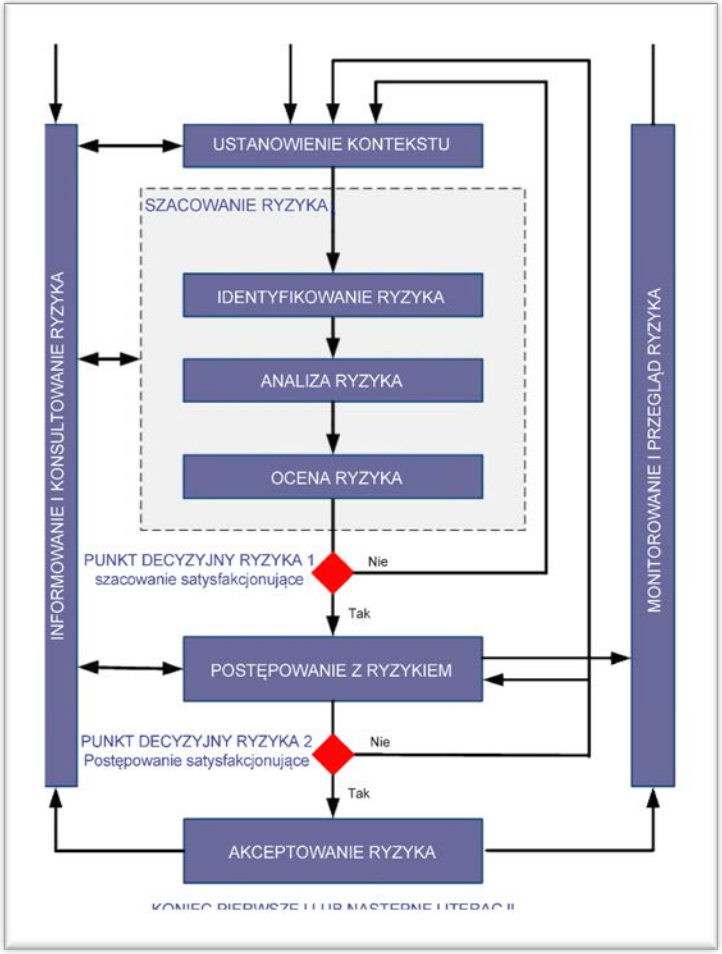
GDPR RISK TRACKER
by lubasz&wspólnicy

Pierwszy krok

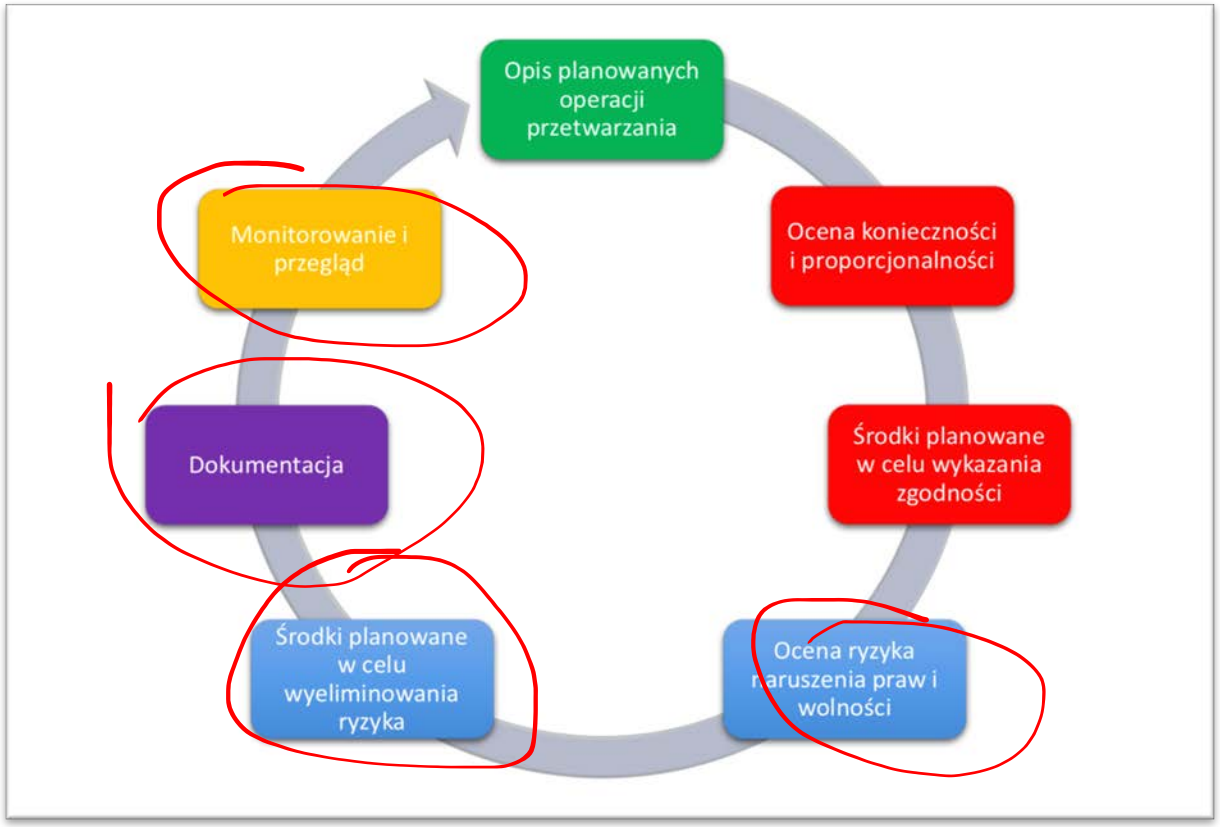
- Mapowanie procesów biznesowych
- Podział na czynności przetwarzania (RCP)
- Ustalenie kontekstu
- Weryfikacja wewnętrzna i zewnętrzna

Przykładowy proces zarządzania bezpieczeństwem informacji wg. ISO 27005 w 6 krokach

1) Ustanowienie kontekstu
2) Identyfikowanie ryzyka
3) Analiza ryzyka
4) Ocena ryzyka
5) Postępowanie z ryzykiem
6) Akceptowanie ryzyka



Kontekstowa analiza ryzyka



Źródło – Wytyczne Grupy roboczej art. 29 dotyczące oceny skutków dla ochrony danych

Rejestr czynności przetwarzania

Jakie czynności przetwarzania?

- Spółka prowadząca działalność handlową – sieć detaliczna sklepów, sklep internetowy, zaopatrywane z magazynu centralnego, z własną logistyką i transportem. Posiada własną flotę kierowców
- Zatrudnia pracowników i B2B oraz pracowników tymczasowych, korzysta z portali LinkedIn oraz pracuj.pl oraz agencji rekrutacyjnych.
- Prowadzi działalność marketingową, za pośrednictwem strony www z analityką i SEO, FB, email-marketingu oraz konkursów i programów lojalnościowych
- Prowadzi politykę weryfikacji dostawców
- Ma monitoring wizyjny w sklepach i samochodach kierowców.

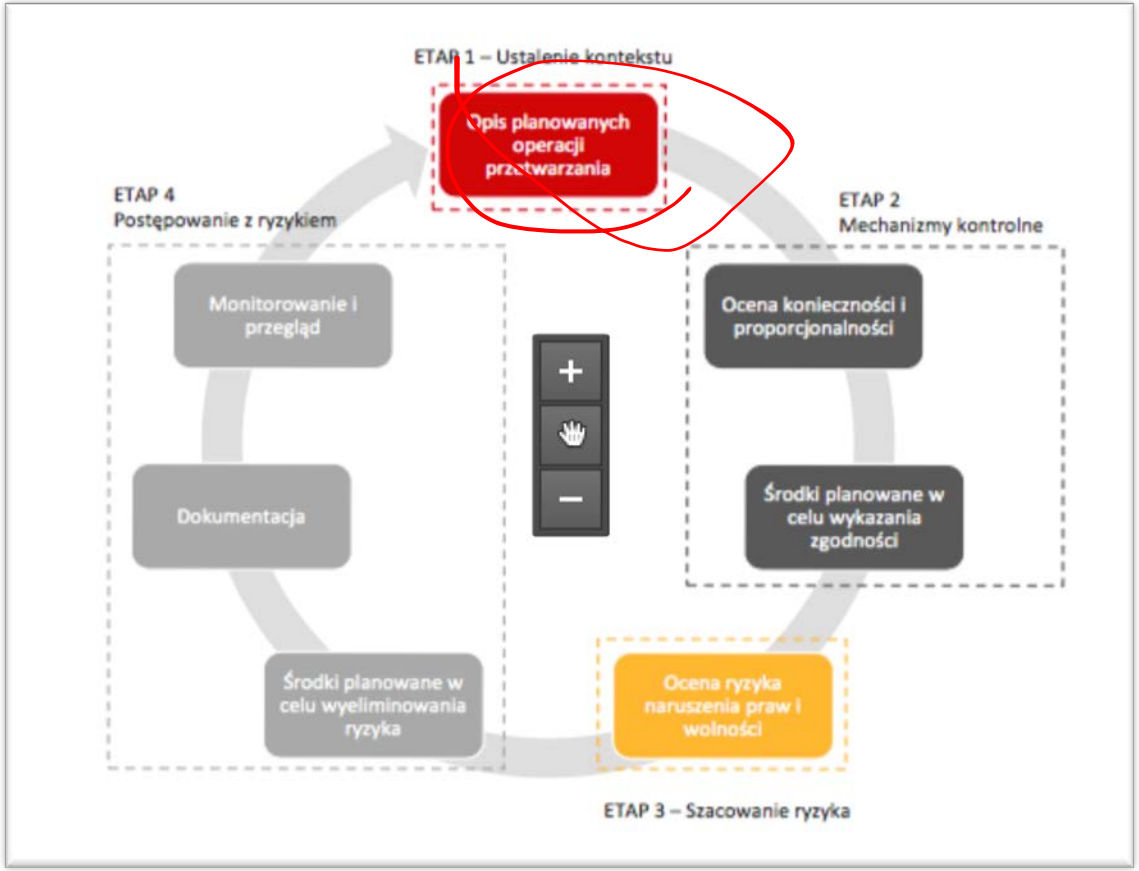
LP.	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*
			Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c			Art.. 30 ust. 1 pkt f	Art.. 30 ust. 1 pkt a
1.	**Rekrutacja pracowników pomocniczych, administracyjnych oraz nauczycieli**	Dyrektor Szkoły	Rekrutacja pracowników	Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych.	Zgoda osób, których dane dotyczą	Kandydaci do pracy	Po zakończeniu procesu rekrutacyjnego	Nie dotyczy
2.	**Prowadzenie rejestru pracowników, akt pracowniczych i ewidencji czasu ich pracy**	Samodzielne stanowisko ds. kadr	Prowadzenie ewidencji pracowników zgodnie z Kodeksem pracy	Pracownicy pomocniczy (recepcjoniści, sprzątaczki, pracownicy gospodarczy), administracyjni oraz nauczyciele	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne, szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem pracy	• Umowa o pracę • Przepis prawa Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 22 z ind. 1 w związku z art. 94 pkt 9a i 9b	Pracownik	50 lat [art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	Nie dotyczy
3.	**Zgłoszenie pracowników i członków ich rodzin do ZUS, aktualizacja zgłoszeń i przekazywanie danych o zwolnieniach**	Samodzielne stanowisko ds. kadr	Zgłoszenia pracownika i członków jego rodziny do ZUS, aktualizacja zgłoszenia oraz przekazywanie informacji o zwolnieniach	Pracownicy pomocniczy (recepcjoniści, sprzątaczki, pracownicy gospodarczy), administracyjni oraz nauczyciele	Dane identyfikacyjne, dane adresowe, dane o Odziale Kasy Chorych oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA - zgłoszenie, ZUS IUA - zmiana danych, ZUS ZWUA - wyrejestrowanie, ZUS ZCNA -zgłoszenie członka rodziny, ZAS - wniosek o ustalenie okresu zasiłkowego, OL-2 - wniosek o kontrolę zaśw. lekarskiego, Z15a - zgłoszenie opieki nad dzieckiem, Z15B - zgłoszenie opieki nad innym członkiem rodziny	• Przepis prawa. Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a	Pracownik	50 lat [art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]	Nie dotyczy

Nazwa podmiotu przetwarzajacego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzajacy)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych srodków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)*	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
					Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt d		Art.. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
Nie dotyczy	Dane nie są przekazywane innym podmiotom	System Kadry. Dokumentacja papierowa.	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	System Kadry. Dokumentacja papierowa.	Zamykane szafy w pomieszczenniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Systemy Kadry. Płatnik. Dokumentacja papierowa.	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy

Rejestr czynności przetwarzania – przykład		
Administrator i jego dane kontaktowe:	**[nazwa spółki], [adres spółki]**	
Dane inspektora ochrony danych lub osoby odpowiedzialnej za ochronę danych osobowych u administratora, jeżeli została wyznaczona:	.....	
Osoba odpowiedzialna za aktualizację rejestru:	.....	
Nazwa procesu (Nazwa czynności przetwarzania):	**Rekrutacja pracowników** *(poszczególne procesy wymagają osobnego ujęcia w analogicznej formie)*	**Numer wpisu: PR/1/2018**
Cel przetwarzania danych:	*Opisać cel przetwarzania w procesie np. wyłonienie spośród kandydatów na określone stanowisko, osoby, która możliwie najdokładniej spełni oczekiwania administratora wobec przyszłego pracownika - pod kątem zarówno umiejętności, kompetencji miękkich, nastawienia do firmy, jak i oczekiwań finansowych.*	
Charakter przetwarzania danych:	*Opisać planowane lub realizowane operacje przetwarzania, rodzaje danych osobowych, które mają być przetwarzane, w tym to czy będą przetwarzane dane wrażliwe* .	
Podstawa przetwarzania	*opisać podstawę przetwarzania, na której oparto proces, np. zgoda kandydata.*	
Kategorie osób, których dane dotyczą	*opisać zaangażowane w proces podmioty* np. ✓ pracownicy obsługujący proces, ✓ kontrahenci obsługujący proces oraz ich pracownicy, ✓ kandydaci do pracy,	
Zakres przetwarzanych danych według kategorii danych: *(wskazano przykładowy zakres)*	Dane identyfikacyjne	• imię (imiona) i nazwisko; • imiona rodziców kandydata do pracy; • data urodzenia kandydata do pracy ; • PESEL
	Dane kontaktowe	• telefon kontaktowy; • adres zameldowania; • adres do korespondencji;
	Dane dotyczące przebiegu kariery i wykształcenia, oczekiwań wobec pracodawcy	• wykształcenie (nazwa szkoły, rok ukończenia szkoły, zawód, specjalność, stopień naukowy, tytuł zawodowy, tytuł naukowy); • wykształcenie uzupełniające (kursy, studia podyplomowe, data ukończenia nauki); • przebieg dotychczasowego zatrudnienia (nazwa pracodawcy, stanowisko pracy, okres zatrudnienia od – do); • oczekiwania finansowe; • wyniki przeprowadzonych testów kompetencji;
	Dane dotyczące dodatkowych uprawnień	• dodatkowe uprawnienia, umiejętności, zainteresowania (np. stopień znajomości języków obcych, prawo jazdy, uprawnienia zawodowe);
Kontekst przetwarzanych danych:	*Opisać wszelkie okoliczności prawne i faktyczne przetwarzania. Przede wszystkim należy oceniać intensywność ingerencji w prywatność danego procesu przetwarzania danych, używanych narzędzi i dostępnej technologii, okoliczności i sposób wykorzystywania założonego rozwiązania i relacji do pozostałych elementów ocennych, w tym celu przetwarzania, a także przesłanek legalizacyjnych. Relewantne mogą również być czas i długość przetwarzania.*	
Kategorie odbiorców / Odbiorcy danych	*Wskazać kategorie odbiorców ewentualnie konkretne podmioty, którym ujawniono lub zostaną ujawnione dane, w tym z państw trzecich, z podziałem na podmioty przetwarzające (np. agencje rekrutacyjne) i innych odbiorców jeśli występują w danym procesie.*	
Współadministrowanie	*Opis współadministrowania, podziału obowiązków oraz dane współadministratora, w tym dane kontaktowe.*	
Transfery danych	*Przekazania danych do państw trzecich lub organizacji międzynarodowych, ze wskazaniem podstawy, na której oparto transfer oraz jeśli jest to przypadek, o którym mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń.*	
Retencja	*Wskazać okresy przechowywania i planowane terminy usunięcia.* *Opisać proces usuwania danych po osiągnięciu celu oraz procedurę ewentualnej zmiany celu.*	
Opis środków technicznych i organizacyjnych	*Opisać zabezpieczenia procesu, fizyczne, organizacyjne, osobowe, techniczne przez pryzmat poufności, integralności i dostępności:* *Np.* *1. Zabezpieczenia organizacyjne:* *a) Upoważnienia do przetwarzania danych* *b) Oświadczenie o zachowaniu poufności* *c) Szkolenie z zakresu ochrony danych* *d) Podpisanie umowy powierzenia* *e) Dokonywanie przeglądów stosowanych procedur*	

GDPR RISK TRACKER
by lubasz&wspólnicy

Analiza ryzyka - iteracje



Źródło – Poradnik „Jak stosować podejście oparte na ryzyku”

Postępowanie z ryzykiem

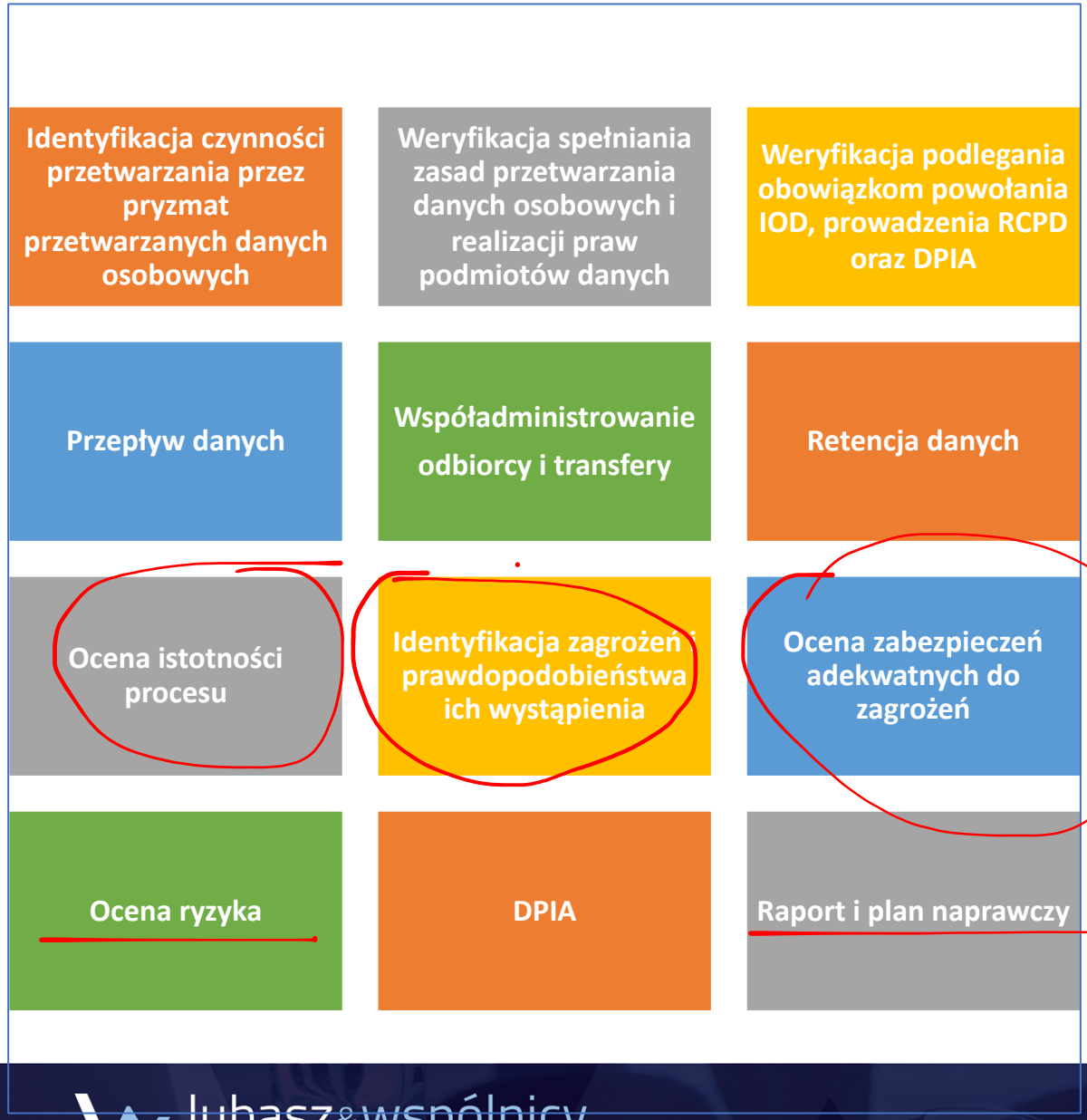
Rysunek 10. Rodzaje postępowania z ryzykiem wg normy ISO/IEC 27005

Źródło – Poradnik „Jak stosować podejście oparte na ryzyku”

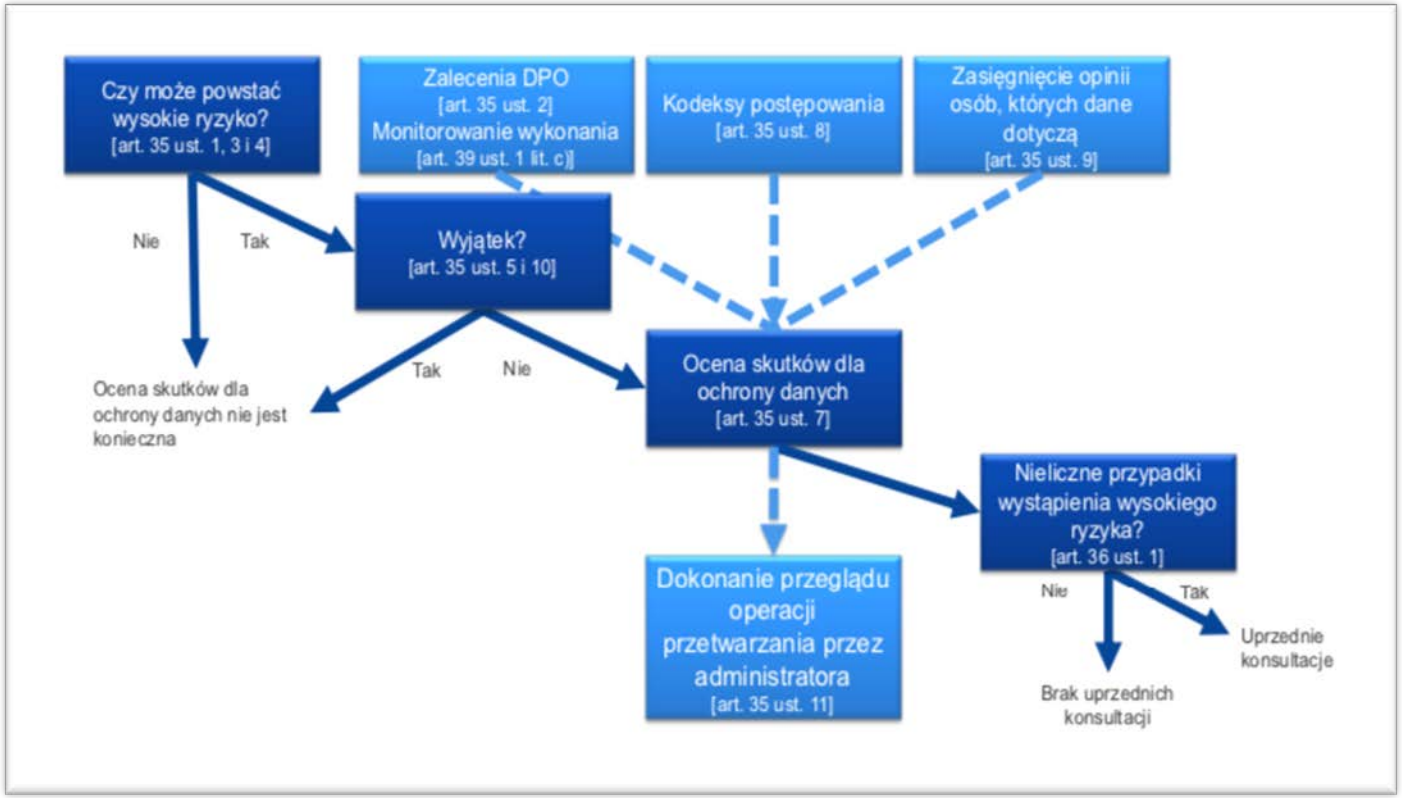
CNIL

identyfikacja czynności przetwarzania rodzącej wysokie ryzyko, uczestników, kontekst przetwarzania	identyfikacja standardów przetwarzania danych, aktywów wykorzystywanych do przetwarzania	identyfikacja przetwarzanych danych, cykl życia danych	weryfikacja celów, legalności, czynności przetwarzania
weryfikacja adekwatności danych (minimalizacja), prawidłowości i możliwości aktualizacji danych	weryfikacja sposobu obsługi praw osób (informacji, zgód, żądań)	identyfikacja istniejących środków ochrony danych	identyfikacja potencjalnych zagrożeń dla osób wskutek (1) nieuprawnionego dostępu, (2) nieautoryzowanej modyfikacji lub zniszczenia
identyfikacja sytuacji grożących naruszeniem ochrony, wraz ze źródłem (insider, człowiek z zewnątrz, technologia, zdarzenia)	ocena prawdopodobieństwa i powagi	plan reakcji – identyfikacja adekwatnych zabezpieczeń	ocena ryzyka szczątkowego

GDPR RISK TRACKER by lubasz&wspólnicy



DPIA - warunki



Źródło – Wytyczne Grupy roboczej art. 29 dotyczące oceny skutków dla ochrony danych

GDPR RISK TRACKER
by lubasz&wspólnicy

Dokumentacja oceny skutków dla ochrony danych

ocena czy operacje przetwarzania są niezbędne oraz proporcjonalne do celów

systematyczny opis planowanych operacji przetwarzania i celów przetwarzania

ocena ryzyka naruszenia praw lub wolności podmiotów danych

środki planowane w celu zaradzenia ryzyku

Dokumentacja uprzednich konsultacji

• Gdy ma to zastosowanie – odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu,

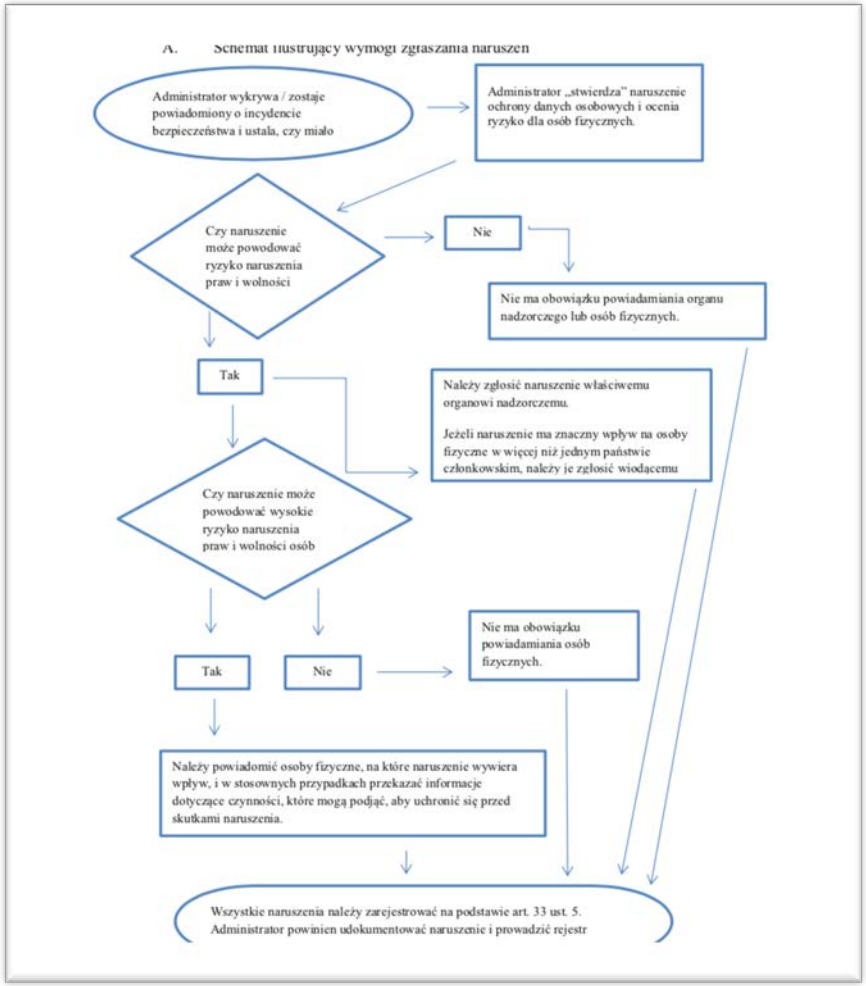
• Cele i sposoby zamierzonego przetwarzania;

• Środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z niniejszym rozporządzeniem;

• Gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;

• Ocenę skutków dla ochrony danych oraz wszelkie inne informacje, których żąda organ nadzorczy.

Dokumentacja naruszeń ochrony danych oraz notyfikacja naruszeń



Źródło – Wytyczne Grupy roboczej art. 29 dotyczące zgłaszania naruszeń ochrony danych

GDPR RISK TRACKER
by lubasz&wspólnicy

Dokumentacja naruszeń ochrony danych oraz notyfikacja naruszeń

Okoliczność naruszenia ochrony danych osobowych

Ewidencja naruszeń

Skutki naruszenia

Notyfikacja do PUODO

Ocena poziomu ryzyka i prawdopodobieństwa

Notyfikacja do podmiotu danych

GDPR RISK TRACKER
by lubasz&wspólnicy

Dokumentacja dopuszczenia do przetwarzania i upoważnień

Administrator określa krąg osób, które mają uprawnienia dostępu do danych i dalszych form ich przetwarzania.

Czynność ta wymaga udokumentowania np. przez określenie zakresu dostępu tak to dokumentów, jak i systemów teleinformatycznych, dopuszczalnych czynności przetwarzania itp.

Nie ma jednak konieczności by odbyła się w wyniku udzielenia upoważnienia. Może to następować przy określaniu zakresu obowiązków, czy ustawieniu dostępu do systemów, po uprzednim przeszkoleniu z zakresu ochrony danych osobowych.

GDPR RISK TRACKER
by lubasz&wspólnicy

Dokumentacja dopuszczenia do przetwarzania i upoważnień

MATRYCA UPOWAŻNIEŃ	DZIAŁ	Kadra zarządzająca						HR	
	STANOWISKO	Dyrektor Generalny	Menadżer Personalny	Dyrektor Administracyjno-Finansowy	Dyrektor Sprzedaży	Dyrektor Łancucha Dostaw	Dyrektor Fabryki	Specjalista Personalny	Specjalista Employer Branding
PROCES	ZAKRES UPOWAŻNIENIA (OPERACJE W PROCESIE)								
REKRUTACJA PRACOWNIKÓW, WSPÓŁPRACOWNIKÓW, STAŻYSTÓW, PRAKTYKANTÓW	gromadzenie/zbieranie/pobieranie	✓							
	organizowanie, porządkowanie, adaptowanie, modyfikowanie, dopasowywanie, łączenie	✓							
	przechowywanie	✓							
	wykorzystywanie, przeglądanie								
	udostępnianie, rozpowszechnianie, ujawnianie poprzez przesyłanie								
	ograniczanie, usuwanie, niszczenie								
REALIZACJA OBOWIĄZKÓW PRACODAWCY W ZWIĄZKU ZE STOSUNKIEM PRACY	gromadzenie/zbieranie/pobieranie								
	organizowanie, porządkowanie, adaptowanie, modyfikowanie, dopasowywanie, łączenie								
	przechowywanie								
	wykorzystywanie, przeglądanie								
	udostępnianie, rozpowszechnianie, ujawnianie poprzez przesyłanie								
	ograniczanie, usuwanie, niszczenie								

GDPR RISK TRACKER
by lubasz&wspólnicy

Dokumentacja powierzeń i poleceń

Prowadzenie rejestru pozwala usystematyzować otrzymywane od administratora polecenia (instrukcje), które mogą wynikać z:
- działania podmiotu przetwarzającego dane na zlecenie administratora,
- działania osoby (np. pracownika) administratora,
- działania osoby (np. pracownika) podmiotu przetwarzającego dane na zlecenie (procesora).

Rejestr poleceń administratora

Dane osoby/podmiotu wykonującego polecenie administratora: [imię/nazwisko/nazwa] [adres siedziby firmy]
Dane inspektora ochrony danych lub osoby odpowiedzialnej za ochronę danych osobowych, jeżeli została wyznaczona: [imię, nazwisko] [numer telefonu]
Osoba odpowiedzialna za aktualizację rejestru: [imię, nazwisko]

1	2	3	3	4	5	6	7	8	9	10	11	12
Numer wpisu	Data wpisu	Oznaczenie administratora	Źródło polecenia (np. umowa, upoważnienie)	Przetwarzanie danych wynika z przepisu prawa (krajowego bądź UE)	Treść polecenia	Zakres polecenia (np. kategorię danych, rodzaj czynności, jaka ma zostać podjęta)	Termin wykonania (o ile został ustalony)	Przyczyny braku możliwości wykonania (jeśli dotyczy)	Administrator poinfromowany	Informacje dodatkowe	Data modyfikacji wpisu	Uwagi
01/2019	[RRRR-MM-DD]	[nazwa / siedziba]	[nazwa / oznaczenie]	TAK / NIE			[RRRR-MM-DD]	Np. z uwagi na możliwości techniczne i organizacyjne	TAK / NIE		[RRRR-MM-DD]	
02/2019	[RRRR-MM-DD]	[nazwa / siedziba]	[nazwa / oznaczenie]	TAK / NIE			[RRRR-MM-DD]	Np. z przyczyn finansowych	TAK / NIE		[RRRR-MM-DD]	
03/2019	[RRRR-MM-DD]	[nazwa / siedziba]	[nazwa / oznaczenie]	TAK / NIE			[RRRR-MM-DD]		TAK / NIE		[RRRR-MM-DD]	

Rejestr powierzeń przetwarzania danych osobowych

Dane administratora: [nazwa; adres siedziby]
Dane inspektora ochrony danych [jeżeli został wyznaczony]: [imię, nazwisko; adres e-mail]
Osoba odpowiedzialna za aktualizację rejestru: [imię, nazwisko]

1	2	3	3	4	5	6	7	8	9	10	11	12
Numer wpisu	Data wpisu	Podmiot przetwarzający	Czy została zawarta umowa powierzenia zgodna z RODO?	Umowa główna, do której odnosi się umowa powierzenia	Okres powierzenia	Zakres powierzonych danych osobowych	Cel przetwarzania danych osobowych	Kontekst przetwarzania danych osobowych	Podpowierzenia podmiotu przetwarzającego	Informacje dodatkowe	Data modyfikacji wpisu	Status

GDPR RISK TRACKER
by lubasz&wspólnicy

Dokumentacja spełnienia przesłanek legalizacyjnych

Weryfikacja i zapewnienie spełnienia przesłanek przetwarzania wskazanych w art. 6 ust. 1 i art. 9 ust. 2 RODO, stanowi podstawę dla procesów przetwarzania.

Analiza administratora powinna być nakierowana na udokumentowanie spełnienia **zasady minimalizacji =** wykazania, że na wybranej i zastosowanej podstawie przetwarzania, w procesie przetwarzał będzie jedynie dane **niezbędne z perspektywy celu przetwarzania**.

GDPR RISK TRACKER
by lubasz&wspólnicy

Dokumentacja transferów danych do państw trzecich

- opis kategorii podmiotów danych oraz kategorii danych ich dotyczących
- opis procesów, w których dochodzi do transferów
- podstawa transferu danych
- ocena poziomu adekwatności ochrony dla instrumentów z art. 46
- charakter transferu
- cele przetwarzania danych i potencjalne alternatywy dla tego sposobu przetwarzania
- szersza dokumentacja odpowiednich zabezpieczeń

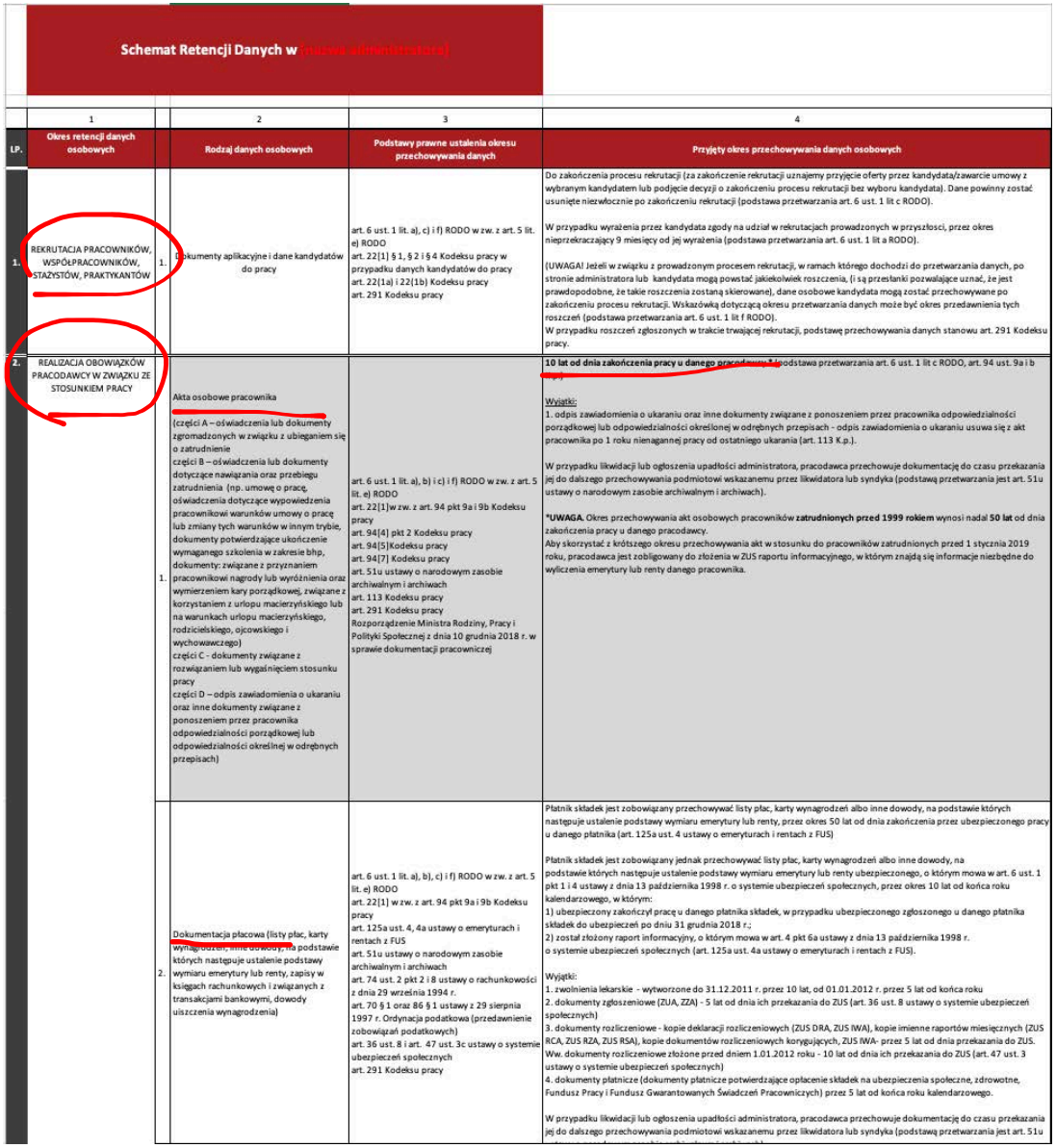
GDPR RISK TRACKER
by lubasz&wspólnicy

Polityka retencyjna

Zgodnie z zasadą ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO) dane osobowe muszą 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.

Zasada ta w korelacji z zasadą celowości determinuje więc czasowe ramy przetwarzania, nakazując przetwarzanie danych przez czas dłuższy niż ten, który wynika z konkretnego celu przetwarzania.

Polityka retencyjna

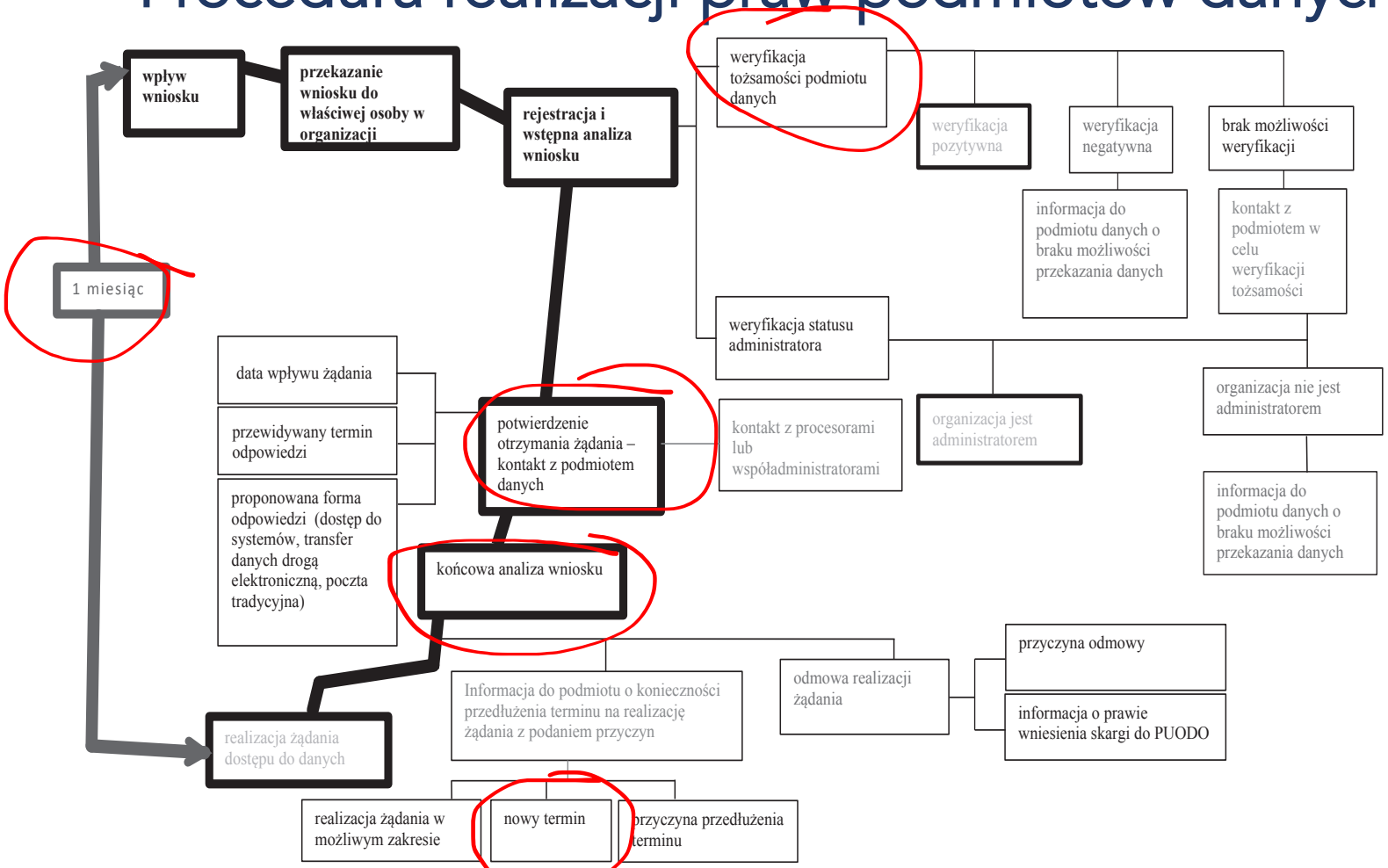


Schemat Retencji Danych w [nazwa administratora]

	1		2	3	4
LP.	Okres retencji danych osobowych		Rodzaj danych osobowych	Podstawy prawne ustalenia okresu przechowywania danych	Przyjęty okres przechowywania danych osobowych
1.	REKRUTACJA PRACOWNIKÓW, WSPÓŁPRACOWNIKÓW, STAŻYSTÓW, PRAKTYKANTÓW	1.	Dokumenty aplikacyjne i dane kandydatów do pracy	art. 6 ust. 1 lit. a), c) i f) RODO w zw. z art. 5 lit. e) RODO art. 22(1) § 1, § 2 i § 4 Kodeksu pracy w przypadku danych kandydatów do pracy art. 22(1a) i 22(1b) Kodeksu pracy art. 291 Kodeksu pracy	Do zakończenia procesu rekrutacji (za zakończenie rekrutacji uznajemy przyjęcie oferty przez kandydata/zawarcie umowy z wybranym kandydatem lub podjęcie decyzji o zakończeniu procesu rekrutacji bez wyboru kandydata). Dane powinny zostać usunięte niezwłocznie po zakończeniu rekrutacji (podstawa przetwarzania art. 6 ust. 1 lit c RODO). W przypadku wyrażenia przez kandydata zgody na udział w rekrutacjach prowadzonych w przyszłości, przez okres nieprzekraczający 9 miesięcy od jej wyrażenia (podstawa przetwarzania art. 6 ust. 1 lit a RODO). [UWAGA! Jeżeli w związku z prowadzonym procesem rekrutacji, w ramach którego dochodzi do przetwarzania danych, po stronie administratora lub kandydata mogą powstać jakiekolwiek roszczenia, (i są przesłanki pozwalające uznać, że jest prawdopodobne, że takie roszczenia zostaną skierowane), dane osobowe kandydata mogą zostać przechowywane po zakończeniu procesu rekrutacji. Wskazówką dotyczącą okresu przetwarzania danych może być okres przedawnienia tych roszczeń (podstawa przetwarzania art. 6 ust. 1 lit f RODO). W przypadku roszczeń zgłoszonych w trakcie trwającej rekrutacji, podstawę przechowywania danych stanowu art. 291 Kodeksu pracy.
2.	REALIZACJA OBOWIĄZKÓW PRACODAWCY W ZWIĄZKU ZE STOSUNKIEM PRACY	1.	Akta osobowe pracownika (części A – oświadczenia lub dokumenty zgromadzonych w związku z ubieganiem się o zatrudnienie części B – oświadczenia lub dokumenty dotyczące nawiązania oraz przebiegu zatrudnienia (np. umowę o pracę, oświadczenia dotyczące wypowiedzenia pracownikowi warunków umowy o pracę lub zmiany tych warunków w innym trybie, dokumenty potwierdzające ukończenie wymaganego szkolenia w zakresie bhp, dokumenty: związane z przyznaniem pracownikowi nagrody lub wyróżnienia oraz wymierzeniem kary porządkowej, związane z korzystaniem z urlopu macierzyńskiego lub na warunkach urlopu macierzyńskiego, rodzicielskiego, ojcowskiego i wychowawczego) części C - dokumenty związane z rozwiązaniem lub wygaśnięciem stosunku pracy części D – odpis zawiadomienia o ukaraniu oraz inne dokumenty związane z ponoszeniem przez pracownika odpowiedzialności porządkowej lub odpowiedzialności określonej w odrębnych przepisach)	art. 6 ust. 1 lit. a), b) i c) i f) RODO w zw. z art. 5 lit. e) RODO art. 22[1]w zw. z art. 94 pkt 9a i 9b Kodeksu pracy art. 94[4] pkt 2 Kodeksu pracy art. 94[5]Kodeksu pracy art. 94[7] Kodeksu pracy art. 51u ustawy o narodowym zasobie archiwalnym i archiwach art. 113 Kodeksu pracy art. 291 Kodeksu pracy Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej	**10 lat od dnia zakończenia pracy u danego pracodawcy** (podstawa przetwarzania art. 6 ust. 1 lit c RODO, art. 94 ust. 9a i b K.p.) Wyjątki: 1. odpis zawiadomienia o ukaraniu oraz inne dokumenty związane z ponoszeniem przez pracownika odpowiedzialności porządkowej lub odpowiedzialności określonej w odrębnych przepisach - odpis zawiadomienia o ukaraniu usuwa się z akt pracownika po 1 roku nienagannej pracy od ostatniego ukarania (art. 113 K.p.). W przypadku likwidacji lub ogłoszenia upadłości administratora, pracodawca przechowuje dokumentację do czasu przekazania jej do dalszego przechowywania podmiotowi wskazanemu przez likwidatora lub syndyka (podstawą przetwarzania jest art. 51u ustawy o narodowym zasobie archiwalnym i archiwach). ***UWAGA.** Okres przechowywania akt osobowych pracowników **zatrudnionych przed 1999 rokiem** wynosi nadal **50 lat** od dnia zakończenia pracy u danego pracodawcy. Aby skorzystać z krótszego okresu przechowywania akt w stosunku do pracowników zatrudnionych przed 1 stycznia 2019 roku, pracodawca jest zobligowany do złożenia w ZUS raportu informacyjnego, w którym znajdą się informacje niezbędne do wyliczenia emerytury lub renty danego pracownika.
		2.	Dokumentacja płacowa (listy płac, karty wynagrodzeń, inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty, zapisy w księgach rachunkowych i związanych z transakcjami bankowymi, dowody uiszczenia wynagrodzenia)	art. 6 ust. 1 lit. a), b), c) i f) RODO w zw. z art. 5 lit. e) RODO art. 22[1] w zw. z art. 94 pkt 9a i 9b Kodeksu pracy art. 125a ust. 4, 4a ustawy o emeryturach i rentach z FUS art. 51u ustawy o narodowym zasobie archiwalnym i archiwach art. 74 ust. 2 pkt 2 i 8 ustawy o rachunkowości z dnia 29 września 1994 r. art. 70 § 1 oraz 86 § 1 ustawy z 29 sierpnia 1997 r. Ordynacja podatkowa (przedawnienie zobowiązań podatkowych) art. 36 ust. 8 i art. 47 ust. 3c ustawy o systemie ubezpieczeń społecznych art. 291 Kodeksu pracy	Płatnik składek jest zobowiązany przechowywać listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty, przez okres 50 lat od dnia zakończenia przez ubezpieczonego pracy u danego płatnika (art. 125a ust. 4 ustawy o emeryturach i rentach z FUS) Płatnik składek jest zobowiązany jednak przechowywać listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty ubezpieczonego, o którym mowa w art. 6 ust. 1 pkt 1 i 4 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, przez okres 10 lat od końca roku kalendarzowego, w którym: 1) ubezpieczony zakończył pracę u danego płatnika składek, w przypadku ubezpieczonego zgłoszonego u danego płatnika składek do ubezpieczeń po dniu 31 grudnia 2018 r.; 2) został złożony raport informacyjny, o którym mowa w art. 4 pkt 6a ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (art. 125a ust. 4a ustawy o emeryturach i rentach z FUS). Wyjątki: 1. zwolnienia lekarskie - wytworzone do 31.12.2011 r. przez 10 lat, od 01.01.2012 r. przez 5 lat od końca roku 2. dokumenty zgłoszeniowe (ZUA, ZZA) - 5 lat od dnia ich przekazania do ZUS (art. 36 ust. 8 ustawy o systemie ubezpieczeń społecznych) 3. dokumenty rozliczeniowe - kopie deklaracji rozliczeniowych (ZUS DRA, ZUS IWA), kopie imienne raportów miesięcznych (ZUS RCA, ZUS RZA, ZUS RSA), kopie dokumentów rozliczeniowych korygujących, ZUS IWA- przez 5 lat od dnia przekazania do ZUS. Ww. dokumenty rozliczeniowe złożone przed dniem 1.01.2012 roku - 10 lat od dnia ich przekazania do ZUS (art. 47 ust. 3 ustawy o systemie ubezpieczeń społecznych) 4. dokumenty płatnicze (dokumenty płatnicze potwierdzające opłacenie składek na ubezpieczenia społeczne, zdrowotne, Fundusz Pracy i Fundusz Gwarantowanych Świadczeń Pracowniczych) przez 5 lat od końca roku kalendarzowego. W przypadku likwidacji lub ogłoszenia upadłości administratora, pracodawca przechowuje dokumentację do czasu przekazania jej do dalszego przechowywania podmiotowi wskazanemu przez likwidatora lub syndyka (podstawą przetwarzania jest art. 51u

GDPR RISK TRACKER
by lubasz&wspólnicy

Procedura realizacji praw podmiotów danych



GDPR RISK TRACKER
by lubasz&wspólnicy

Dokumentacja realizacji praw podmiotów danych

Administrator powinien móc wykazać m.in.:

- otrzymanie żądania podmiotu danych,
- weryfikację tożsamości osoby, której udziela się informacji,
- dochowanie terminów realizacji żądania,
- że prawo do uzyskania kopii nie wpływa niekorzystnie na prawa i wolności innych osób,
- że poinformował administratorów przetwarzających te dane osobowe o żądaniu podmiotu danych ich usunięcia,
- wyjątki uprawniające administratora do odmowy usunięcia danych,
- pozytywne przeprowadzenie testu równowagi na podstawie art. 21 ust. 1 RODO.

GDPR RISK TRACKER by lubasz&wspólnicy

Polityka ochrony danych

W RODO nie znajdujemy **szczegółowych wymogów co do zakresu merytorycznego lub formy dokumentacji ochrony danych** w postaci polityki ochrony danych. Prawodawca unijny pozostawił w tym względzie swobodę administratorom, podkreślając jedynie, że dokumenty te mogą służyć do realizacji zasady rozliczalności, czyli wykazania przez administratora spełniania wymogów wynikających z rozporządzenia.

GDPR RISK TRACKER by lubasz&wspólnicy

GDPR RISK TRACKER by lubasz&wspólnicy

LISTA CZYNNOŚCI SŁOWNIKI MÓJ PROFIL

ADMINISTRATOR PRZYKŁADOWY

Dodaj nową czynność

+

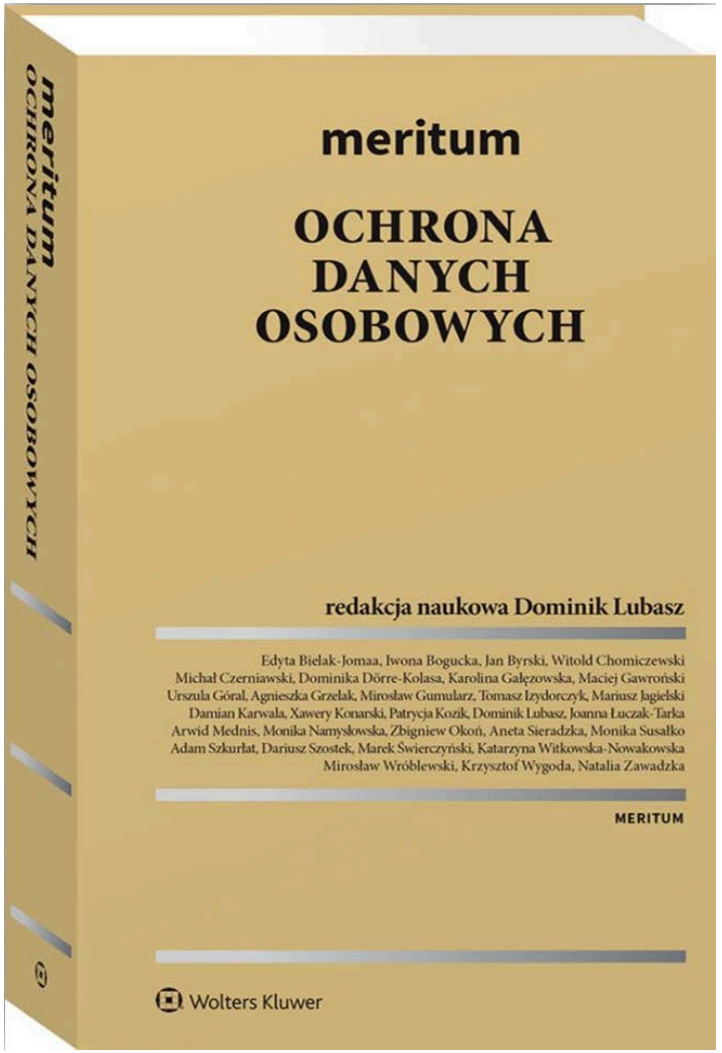
PRACA ZDALNA

Autor: **Dominik Lubasz**
Utworzono: **27.03.2020**
Ukończono: **100%**

GDPR RISK TRACKER
by lubasz&wspólnicy

lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH


GDPR
RISK TRACKER
by lubasz&wspólnicy
STRONA GŁÓWNA
O APLIKACJI
OFERTA
KONTAKT
UTWÓRZ KONTO
ZALOGUJ SIĘ
Wybierz ofertę dla Ciebie
już od 39 zł*
cena wybranego pakietu: 39,00 zł netto
(47,97 zł brutto)
LITE
Limit użytkowników: 1
Abonament miesięczny
Abonament półroczny
Abonament roczny
już od 59 zł*
cena wybranego pakietu: 59,00 zł netto
(72,57 zł brutto)
NORMAL
Limit użytkowników: 4
Abonament miesięczny
Abonament półroczny
Abonament roczny
już od 99 zł*
cena wybranego pakietu: 99,00 zł netto
(121,77 zł brutto)
PRO
Limit użytkowników: 9
Abonament miesięczny
Abonament półroczny
Abonament roczny
*Podane ceny, są cenami netto
lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH



PORTALODO

PORTALPRAWAIT

lubasz&wspólnicy

KANCELARIA RADCÓW PRAWNYCH

pl-pl.facebook.com/lubaszwspolnicy/

pl.linkedin.com/company/lubasz-i-wspolnicy-law-firm

twitter.com/liwlegal