SOCIETE GENERALE
Insurance

POLITYKA OCHRONY DANYCH OSOBOWYCH SGIP

Spis treści

SOCIETE GENERALE
Insurance

1. RODO ma wpływ na Societe Generale Insurance Polska (SGIP) [1]

1.1. Czym jest RODO?

Ogólne rozporządzenie o ochronie danych (RODO) odnosi się do europejskiego rozporządzenia nr 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, które weszło w życie 25 maja 2018 r.

RODO uchyla dyrektywę 95/46/WE, która wcześniej regulowała kwestię ochrony danych osobowych. Dogłębnie odnawia ramy prawne ochrony danych osobowych.

RODO chroni dane osób fizycznych wykorzystywane w procesach przetwarzania związanych z działalnością organizacji (przedsiębiorstw, władz lokalnych itp.).

Uzupełnia ono i wzmacnia istniejące wymagania krajowe:

- Wzmacnia miejsce osoby fizycznej w centrum prawnego i technicznego systemu ochrony danych i oferuje jej nowe prawa lub gwarancje, aby umożliwić jej lepszą kontrolę nad jej danymi.

- Wprowadza odpowiedzialność przedsiębiorstw przetwarzających dane osobowe, w tym podmiotów przetwarzających. Każde z nich, na swoim poziomie, musi chronić dane osobowe poprzez wdrożenie środków organizacyjnych i technicznych dostosowanych do zagrożeń dla prywatności osób, których dane dotyczą, w odniesieniu do istniejących lub nowych operacji przetwarzania.

- Ratyfikuje potrzebę śledzenia działań i środków kontroli, jak również bezpieczeństwa danych osobowych (obowiązek prowadzenia rejestru) i zapewnia ramy dla nowych praktyk technologicznych (profilowanie, sztuczna inteligencja).

- Zapewnia ramy dla przetwarzania i przekazywania danych osobowych do krajów spoza Unii Europejskiej.

- Rozszerza zakres wymiany z organami nadzorczymi (obowiązek powiadamiania o naruszeniu danych osobowych, wcześniejsze konsultacje w przypadku operacji przetwarzania mogących powodować wysokie ryzyko), a także wzmacnia kontrolę regulatora i jego uprawnienia do nakładania sankcji.

RODO zapewnia ramy dla:

- **gromadzenia,**
- **wykorzystywania,**
- **oraz przechowywania/usuwania danych osobowych.**

1.2. Co stanowi RODO?

RODO przewiduje szereg podstawowych zasad, które wymagają, aby dane osobowe były:

- przetwarzane na jednej z sześciu podstaw prawnych przewidzianych w RODO (zasada zgodności z prawem, §3.1.2),

[1] SGIP rozumiane jako Sogecap Oddział w Polsce i/lub Sogessur Oddział w Polsce

- przetwarzane w sposób przejrzysty dla osób, których dane dotyczą, którym należy udzielić informacji o przetwarzaniu ich danych w momencie ich gromadzenia (zasada przejrzystości, §3.2),

- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji, §3.5.1),

- przechowywane przez okres nie dłuższy niż jest to konieczne do osiągnięcia celu, dla którego zostały zgromadzone (zasada ograniczenia przechowywania, §3.1.3),

- zabezpieczone przed ryzykiem naruszenia poufności, integralności i dostępności, z uwzględnieniem w szczególności rodzaju danych (wrażliwe lub nie), przewidywanych zagrożeń lub kontekstu (zasada bezpieczeństwa przetwarzania, §3.4).

Najważniejsze informacje - co musisz wiedzieć

RODO chroni dane osób fizycznych, i tylko osób fizycznych.

Dane osób prawnych nie są objęte ochroną na podstawie przepisów RODO.

1.3. Co to są dane osobowe?

Zgodnie z RODO dane osobowe to wszelkie dane lub informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania, bezpośrednio lub pośrednio, osoby fizycznej. Aby uprościć ich identyfikację i klasyfikację, dane osobowe są często kategoryzowane w następujący sposób:

- tożsamość, przykłady: nazwisko, imię, data urodzenia, itp.

- życie osobiste, przykłady: stan cywilny, skład gospodarstwa domowego, dane z mediów społecznościowych, itp.

- życie zawodowe, przykłady: zawód, doświadczenie zawodowe, zawodowe dane kontaktowe, itp.

- informacje ekonomiczne i finansowe, przykłady: dochód, majątek, wskaźnik zadłużenia, itp.

- dane dotyczące logowania, przykłady: adres IP, numer IMEI telefonu, adres MAC komputera, itp.

- dane lokalizacyjne, przykłady: inteligentny samochód, geolokalizacja telefonu, itp.

- ...

Niektóre dane są uważane za wrażliwe (wymienione w artykułach 9 i 10 RODO lub określone jako takie przez państwo członkowskie UE). Ich przetwarzanie podlega zasadzie zakazu przetwarzania z pewnymi wyjątkami i pod pewnymi warunkami.

Dotyczy to danych osobowych odnoszących się do:

- pochodzenia rasowego lub etnicznego,

SGIP nigdy nie przetwarza tych danych w ramach swojej działalności,

- poglądów politycznych,

SGIP nigdy nie przetwarza tych danych w ramach swojej działalności,

- przekonań religijnych lub filozoficznych,

SGIP nigdy nie przetwarza tych danych w ramach swojej działalności,

- przynależności do związków zawodowych,

SGIP nigdy nie przetwarza tych danych w ramach swojej działalności,

- przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej,

SGIP nigdy nie przetwarza tych danych w ramach swojej działalności,

- stanu zdrowia osoby,

SGIP może przetwarzać te dane w kontekście subskrypcji i/lub obsługi roszczeń związanych z zawartymi umowami ubezpieczenia,

- dane dotyczące życia seksualnego lub orientacji seksualnej osoby fizycznej,

SGIP nigdy nie przetwarza tych danych w ramach swojej działalności,

- dane osobowe związane z wyrokami skazującymi,

SGIP może przetwarzać te dane w ramach AML-CFT lub zawierania umów ubezpieczenia komunikacyjnego.

Dane, które w momencie gromadzenia są anonimowe lub zostały poddane nieodwracalnemu procesowi anonimizacji, nie są danymi osobowymi, ponieważ na ich podstawie nie jest możliwa identyfikacja osoby fizycznej.

Z kolei dane pseudonimizowane (odwracalny proces anonimizacji, np. zastąpienie nazwiska/imienia niepowtarzalnym identyfikatorem) pozostają danymi osobowymi, o ile nadal można zidentyfikować osoby fizyczne.

Najważniejsze informacje - co musisz wiedzieć

Niektóre dane osobowe są bardziej wrażliwe niż inne, a ich przetwarzanie podlega ograniczeniom i warunkom.

Jeżeli dane zostały zanonimizowane i nie można ich już powiązać z konkretną osobą, wówczas nie są to już dane osobowe.

1.4. Wyzwania stojące przed SGIP

Działalność SGIP jest związana z wykorzystywaniem dużej ilości danych osobowych, z których część ma charakter wrażliwy, w związku z czym SGIP jest zobowiązane do przestrzegania obowiązujących przepisów prawnych i regulacji.

W tym kontekście ochrona osób fizycznych w zakresie gromadzenia i przetwarzania danych osobowych jest prawem podstawowym i kwestią strategiczną, niezbędną dla zachowania zaufania klientów, partnerów i pracowników każdego podmiotu, jak również ochrony reputacji SGIP.

W związku z tym, nieprzestrzeganie postanowień RODO, naraża SGIP i Grupę SOGECAP na kary ze strony Urzędu Ochrony Danych Osobowych (PUODO) w wysokości do 4% całkowitego rocznego światowego obrotu, lub 20 milionów euro (zastosowanie ma kwota wyższa).

SGIP jest również narażone na ewentualne pozwy cywilne ze strony osób, których dane dotyczą, a zatem również na ryzyko utraty reputacji.

Najważniejsze informacje - co musisz wiedzieć

Odpowiedzialność za ochronę danych spoczywa zarówno na poziomie każdego podmiotu Grupy SOGECAP wobec jego lokalnego Urzędu Ochrony Danych Osobowych, jak i na poziomie szefa Grupy SOGECAP. W związku z tym, uchybienie w ochronie danych osobowych w jednej ze spółek zależnych/oddziałów może mieć konsekwencje dla całej Grupy SOGECAP.

1.5. Cele polityki ochrony danych osobowych

Polityka ochrony danych osobowych jest częścią strategii kontroli ryzyka regulacyjnego i operacyjnego SGIP.

Jest ona również zgodna z Kodeksem Société Générale, który w swojej Księdze B zawiera Rozdział 3 - Zasady dotyczące danych, w którym Sekcja 2 wyszczególnia organizację, środki i zasady związane z ochroną danych osobowych. Polityka ochrony danych osobowych szczegółowo określa sposób wdrożenia zasad zawartych w Kodeksie Société Générale.

Jest ona poddawana corocznemu przeglądowi i aktualizowana w przypadku wystąpienia znaczącego zdarzenia.

Niniejszy dokument podsumowuje obowiązki wynikające z RODO. Przedstawia również ład korporacyjny i procedury, które SGIP wdrożyło w celu zapewnienia zgodności z rozporządzeniem. Określa on przewodnie zasady ochrony danych osobowych.

Polityka ta wbudowuje się w ramy normatywne SGIP (procedury, procedury operacyjne).

Najważniejsze informacje - co musisz wiedzieć

Polityka ochrony danych osobowych określa zasady ochrony danych osobowych w SGIP. Uzupełniają ją procedury i standardowe procedury operacyjne.

1.6. Zakres polityki

RODO ma zastosowanie do wszystkich organizacji (firm, administracji, stowarzyszeń) mających siedzibę na terytorium państwa członkowskiego Unii Europejskiej. Tym samym RODO ma zastosowanie do wszystkich spółek zależnych i oddziałów Grupy SOGECAP mających siedzibę w krajach UE, w tym do SGIP.

RODO ma również zastosowanie do organizacji, które nie mają siedziby w UE, w przypadku sprzedaży produktów i usług osobom w UE.

Zasady tej polityki obowiązują, z mocy prawa i/lub na mocy porozumień, wszystkie podmioty przetwarzające współpracujące z SGIP.

Najważniejsze informacje - co musisz wiedzieć

Polityka ochrony danych osobowych ma zastosowanie do wszystkich europejskich podmiotów należących do Grupy SOGECAP oraz do podmiotów spoza UE, które przetwarzają dane osób z Unii Europejskiej.

2. Podmioty zaangażowane w ochronę danych osobowych w ramach SGIP

Poszczególne podmioty zaangażowane w ochronę danych osobowych w ramach SGIP zostały zidentyfikowane w rejestrze przetwarzania danych lub w wewnętrznych procedurach dotyczących przetwarzania danych osobowych. Każda czynność przetwarzania jest powiązana ze strukturą organizacyjną i osobą prawną.

Ponadto, podczas tworzenia lub modyfikacji operacji przetwarzania danych osobowych, mobilizowane są inne zainteresowane strony w celu wsparcia projektu lub przekazania swojej wiedzy specjalistycznej w zakresie ochrony danych osobowych.

Interesariusze ochrony danych wymienieni w niniejszej polityce mają te same role i obowiązki, które są wymienione dla tych interesariuszy w Kodeksie Société Générale. Interesariusze ochrony danych i ich role dzielą się na dwie linie obrony:

- Linia obrony 1: działy biznesowe, które są odpowiedzialne za przetwarzanie związane z ich działalnością. Towarzyszą im funkcje wspierające, które pomagają "właścicielom" przetwarzania: dział prawny, bezpieczeństwa itp.,

- Linia obrony 2: Inspektor Ochrony Danych (IOD), który wspiera, nadzoruje i monitoruje działania działów biznesowych (patrz §2.2).

Najważniejsze informacje - co musisz wiedzieć

Linie biznesowe są w pełni odpowiedzialne za kompletność rejestru przetwarzania danych osobowych w obszarze swojej działalności, za zgodność swoich operacji przetwarzania z RODO oraz za udokumentowanie zgodności z RODO.

Inspektor ochrony danych wspiera linie biznesowe i sprawdza adekwatność zgromadzonych informacji.

2.1. Linia obrony 1 - Linie biznesowe są odpowiedzialne za przetwarzanie danych osobowych związanych z ich działalnością

Interesariusze biznesowi (kierownicy produktów, kierownicy projektów, kierownicy aplikacji itp.), którzy wdrażają przetwarzanie danych osobowych, są odpowiedzialni, jako pierwsza linia obrony, za zgodność ich przetwarzania z rozporządzeniem RODO oraz za zgodność z systemami i procedurami SGIP w tym zakresie.

Pierwsza linia obrony składa się w ramach działów biznesowych głównie z kierowników i właścicieli przetwarzania, których wspierają eksperci.

Pracownicy pierwszej linii obrony są odpowiedzialni za:

- Stosowanie zasad RODO i niniejszej polityki podczas prowadzenia swoich projektów.
- Zapewnienie, że rejestr czynności przetwarzania jest aktualizowany w zakresie ich działu lub pionu, aby zapewnić, że jest on zawsze aktualny.
- Przeprowadzanie analiz i badań wymaganych przez RODO związanych z operacjami przetwarzania, które wdrażają, oraz wnioskowanie o wdrożenie odpowiednich środków bezpieczeństwa.
- Zwracanie się o poradę do inspektora ochrony danych w przypadku pytań, wątpliwości lub trudności napotkanych w związku z przetwarzaniem danych osobowych, które wdrażają lub obsługują.
- Informowanie inspektora ochrony danych o wykrytych niezgodnościach z RODO, jak również w przypadku zmian w narzędziach i/lub metodach mających wpływ na przetwarzanie danych osobowych w ramach ich działu.

2.1.1. Dyrektorzy, którzy są odpowiedzialni za operacje przetwarzania wykonywane w ramach ich działu

W ramach swoich obowiązków każdy dyrektor jest odpowiedzialny za zgodność z RODO operacji przetwarzania przeprowadzonych w ramach jego działu, zgodnie z rejestrem czynności przetwarzania danych osobowych.

Obowiązkiem każdego dyrektora jest również wdrażanie zaleceń udzielonych przez inspektora ochrony danych:

- w przypadku każdej nowej operacji przetwarzania danych osobowych,

- w przypadku każdej zmiany w istniejącej operacji przetwarzania danych osobowych,

- w przypadku wystąpienia incydentu ochrony danych osobowych.

Jeśli nie jest możliwe wdrożenie zaleceń IOD, sprawa może zostać przekazana do arbitrażu Dyrektorowi Oddziału lub innemu organowi, jeśli wymaga tego poziom ryzyka.

2.1.2. Właściciele procesu, odpowiedzialni za zgodność operacji przetwarzania podlegających ich kontroli

Każda operacja przetwarzania danych osobowych zarejestrowana w rejestrze czynności przetwarzania danych osobowych ma powiązanego właściciela przetwarzania, będącego dyrektorem lub podlegającego dyrektorowi. Właściciel operacji przetwarzania jest osobą najlepiej wykwalifikowaną do opisywania i aktualizowania operacji przetwarzania oraz do odpowiadania na pytania Urzędu Ochrony Danych w przypadku skargi lub kontroli. Występuje on w roli eksperta.

Właściciele procesów przetwarzania są, w ramach pierwszej linii obrony, odpowiedzialni za operacyjne wdrożenie zasad niniejszej polityki.

W szczególności, są oni odpowiedzialni za ocenę ryzyka, jakie ich przetwarzanie może generować dla osób, których dane dotyczą oraz za przeprowadzenie niezbędnych analiz. Analizy te umożliwiają pomiar poziomu ryzyka nieodłącznego dla operacji przetwarzania oraz określenie ewentualnych działań ograniczających ryzyko, które należy wdrożyć.

2.1.3 Funkcje wspierające wspomagają właścicieli procesów przetwarzania: Dział Prawny, Bezpieczeństwo IT itp.

Kierownik odpowiedzialny za zakupy w SGIP jest również odpowiedzialny za kwestie ochrony danych w procesie zakupów. Zapewnia, że nowe lub renegocjowane umowy o podwykonawstwo zawierają klauzule i załączniki dotyczące ochrony danych osobowych i bezpieczeństwa zgodnie z obowiązującymi przepisami i praktykami Grupy w tym zakresie.

Dział prawny jest odpowiedzialny za negocjacje i sporządzanie klauzul dotyczących danych osobowych w umowach. Jest odpowiedzialny za monitorowanie prawnych i regulacyjnych wymogów związanych z ochroną danych osobowych. Określa prawny lub regulacyjny okres retencji danych osobowych. Określa, sporządza lub zatwierdza noty prawne, które muszą znajdować się we wszystkich dokumentach przedumownych i umownych stosowanych w ramach SGIP. Wreszcie, zapewnia wsparcie prawne dla linii biznesowych podczas tworzenia lub modyfikowania operacji przetwarzania.

Kierownik ds. bezpieczeństwa systemów informatycznych ma duży udział w zapewnieniu zgodności SGIP z RODO, ponieważ wspiera linie biznesowe i doradza im w zakresie środków technicznych służących ochronie danych osobowych, a w razie potrzeby wdraża te środki.

2.2. Linia obrony 2 - zainteresowane strony, które wspierają i nadzorują zgodność operacji przetwarzania danych

Do głównych zadań drugiej linii obrony (LOD2) należy:

- zapewnienie, że mechanizmy ochrony danych w SGIP są zgodne z przepisami,

- zdefiniowanie i zapewnienie walidacji mechanizmów operacyjnych związanych z zarządzaniem danymi osobowymi w SGIP,

- wspieranie departamentów SGIP we wszystkich kwestiach związanych z ochroną danych,
- zarządzanie wnioskami o wykonanie praw wynikających z RODO oraz naruszeniami ochrony danych osobowych mającymi wpływ na SGIP,
- kierowanie i koordynowanie prac związanych z identyfikacją procesów przetwarzania danych osobowych w SGIP oraz ich nadzorowaniem, w tym w szczególności przeprowadzanie analiz i ocen skutków wymaganych przez RODO, a także monitorowanie planów działania związanych z tymi analizami,
- bycie punktem kontaktowym dla organów nadzorczych w przypadku skargi lub kontroli,
- monitorowanie działań w zakresie ochrony danych za pomocą wskaźników ryzyka.

Grupa SOGECAP utworzyła drugą linię obrony w celu zarządzania ochroną danych w ramach Grupy:

- Inspektor Ochrony Danych Grupy SOGECAP (zwany dalej ASSU DPO), który zapewnia nadzór funkcjonalny nad inspektorami lub korespondentami ochrony danych podmiotów międzynarodowych Grupy SOGECAP,
- Inspektorzy Ochrony Danych (IOD) lub Korespondenci Ochrony Danych (DPC) wyznaczeni na poziomie spółek zależnych i oddziałów oraz zgłoszeni w razie potrzeby zgodnie z obowiązującymi przepisami do właściwych organów ochrony danych.

Aby zapewnić efektywność ich misji jako drugiej linii obrony, IOD/DPC polegają na pierwszej linii obrony, która przyczynia się do zgodności systemu ochrony danych.

Zgodność z RODO jest częścią systemu ciągłej i okresowej kontroli ustanowionej w SGIP.

2.2.1. Inspektor ochrony danych ASSU, jako podmiot prowadzący politykę ochrony danych Grupy SOGECAP

ASSU DPO musi zapewnić, w ramach obszaru, za który jest odpowiedzialny, zgodność z RODO. Musi on być zaangażowany, w odpowiedni i terminowy sposób, we wszystkie sprawy związane z ochroną danych osobowych.

Cel ten osiąga się głównie za pomocą misji opisanych poniżej:

- zapewnienie ogólnego zarządzania systemem ochrony danych i zagwarantowanie spójności systemów w skonsolidowanym obszarze wszystkich podmiotów Grupy SOGECAP,
- weryfikacja realizacji niniejszej polityki,
- ostrzeganie administratora danych o wszelkich naruszeniach lub niezgodnościach z niniejszą polityką,
- nadzorowanie poszczególnych IOD i DPC,
- zapewnienie wdrożenia planu stałej kontroli systemu ochrony danych osobowych, który będzie stosowany przez każdy podmiot z Grupy SOGECAP,
- określenie i wdrożenie planu szkoleń, podnoszenia świadomości i komunikacji dla wszystkich osób zaangażowanych w ochronę danych osobowych w Grupie,
- kierowanie siecią korespondentów ds. zgodności i zapewnienie koordynacji działań z liniami biznesowymi i funkcjami w swojej jednostce,
- doradzanie administratorowi, właścicielom linii biznesowych przetwarzającym dane, podmiotom przetwarzającym dane oraz pracownikom, którzy przetwarzają dane osobowe,
- kierowanie i koordynowanie pracami nad ochroną danych osobowych, w tym oceną skutków dla ochrony danych,
- zapewnienie właściwego prowadzenia i aktualizacji rejestru czynności przetwarzania,

- odpowiadanie na reklamacje oraz na wnioski osób, których dane dotyczą, dotyczące wykonywania ich praw,
- badanie i dokumentowanie przypadków naruszenia ochrony danych osobowych, a w razie potrzeby zgłaszanie ich do organu ochrony danych,
- bycie punktem kontaktowym dla organów nadzorczych w przypadku skarg, wniosków lub kontroli,
- zapewnienie właściwej dokumentacji działań prowadzonych w kontekście zarządzania ochroną danych osobowych (opinie IOD, zalecenia, kontrola realizacji planów działania itp.).

2.2.2. IOD/DPC podmiotów międzynarodowych, odpowiedzialni za ochronę danych w ramach swojego podmiotu

Inspektor ochrony danych w SGIP wykonuje te same zadania, co ASSU DPO w ramach Grupy SOGECAP. Pod nadzorem funkcjonalnym ASSU DPO koordynuje działania w sprawach, które tego wymagają.

Jego zadania w tym obszarze są podobne do zadań ASSU DPO, któremu podlega funkcjonalnie: zapewnia zgodność swojej jednostki z RODO i obowiązującymi lokalnie przepisami dotyczącymi ochrony danych osobowych oraz wdraża politykę ochrony danych osobowych oraz związane z nią procedury.

2.3. Organy i funkcjonowanie systemu ochrony danych osobowych

Grupa SOGECAP ustanowiła strukturę zarządzania swoim systemem ochrony danych, która obejmuje kilka komitetów, których członkowie, częstotliwość i cele zostały opisane poniżej.

Na czele tych komitetów stoi ASSU DPO.

2.3.1. Komitety wewnętrzne grupy SOGECAP

Komitet strategiczny ds. RODO
Komitet ten zbiera się ad hoc, gdy pojawiają się kwestie, które należy skierować do Zarządu. DPO i Dyrektor ds. Zgodności przedstawiają postępy we wdrażaniu RODO i obszary ryzyka związane z ochroną danych Komitetowi Wykonawczemu Grupy SOGECAP, jak również główne wskaźniki ilościowe i jakościowe potrzebne do podejmowania decyzji.

Komitet ds. ochrony danych osobowych
Komitet ten gromadzi, co miesiąc, Sekretarza Generalnego, przedstawicieli Departamentu Prawnego i Departamentu Zgodności, w tym Departamentu Ochrony Danych, członków Komitetu Wykonawczego odpowiedzialnych za rozwój działalności, Dyrektora Marketingu i Dyrektora DATA HUB, w celu omówienia kwestii związanych z wykorzystaniem danych do następujących celów:

- rozwój działalności, zarówno w ramach Grupy SOGECAP, jak i we współpracy z dystrybutorami,
- poprawa wiedzy o klientach, zarówno w ramach Grupy SOGECAP, jak i we współpracy z dystrybutorami.

W zależności od porządku obrad mogą być zapraszani inni uczestnicy.

Komitety z udziałem IOD/DPC spółek zależnych i oddziałów Grupy SOGECAP
Komitet IOD/DPC ds. ochrony danych osobowych Grupy SOGECAP ma na celu informowanie i dyskutowanie z inspektorami ochrony danych i DPC o kwestiach związanych z ochroną danych osobowych. W szczególności kieruje wdrażaniem RODO w spółkach zależnych poprzez reagowanie na problemy, z którymi się one borykają.

Komitet ten, któremu przewodniczy ASSU DPO, zrzesza inspektorów ochrony danych i DPC. Posiedzenia odbywają się co dwa miesiące.

Kwartalny komitet ds. Compliance
ASSU DPO i SGIP DPO biorą udział raz na kwartał w spotkaniach komitetu ds. Compliance. Podczas spotkania SGIP DPO prezentuje najważniejsze kwestie dotyczące ochrony danych osobowych w oddziale.

2.3.2. Komitety zewnętrzne w stosunku do grupy SOGECAP

Komitet DPO grupy SOCIETE GENERALE
ASSU DPO bierze udział w spotkaniach komitetu, które odbywają się co miesiąc i mają na celu nadzorowanie i informowanie lokalnych IOD i DPC Grupy SOCIETE GENERALE.

Dwustronne spotkania ASSU DPO / IOD dystrybutorów
ASSU DPO organizuje regularne spotkania, wymiany z IOD swoich głównych dystrybutorów.

Celem tych spotkań, odbywających się co dwa miesiące, jest wymiana poglądów na temat bieżących wydarzeń lub konkretnych tematów będących przedmiotem wspólnego zainteresowania.

3. Główne wyzwania związane z ochroną danych osobowych

3.1. Nadzór nad przetwarzaniem danych osobowych

3.1.1. Posiadanie aktualnego rejestru czynności przetwarzania danych w celu uzyskania wyczerpującej wiedzy na temat operacji przetwarzania dokonywanych przez SGIP

Rejestr czynności przetwarzania danych zawiera wykaz i opis wszystkich operacji przetwarzania danych osobowych dokonywanych przez SGIP. Musi on być aktualizowany i w każdej chwili może być przeglądany przez organy nadzoru. Każda operacja przetwarzania danych osobowych musi zostać wpisana do rejestru czynności przetwarzania z kompletem informacji przed jej pierwszym wykonaniem.

W rejestrze wyszczególnia się istotne cechy każdej operacji przetwarzania. W szczególności rejestr ten musi zawierać co najmniej następujące informacje dotyczące każdej operacji przetwarzania:

- imię i nazwisko oraz dane kontaktowe właściciela procesu przetwarzania, tj. osoby, która najlepiej potrafi odpowiedzieć na pytania dotyczące przetwarzania i przetwarzanych danych,
- cele przetwarzania (np. wykonanie umów ubezpieczenia),
- podstawa prawna przetwarzania i jej uzasadnienie (patrz §3.1.2 poniżej),
- opis kategorii osób, których dane dotyczą (np. klienci, potencjalni klienci, pracownicy, osoby poszukujące pracy) oraz kategorii danych osobowych (np. dane identyfikacyjne, dane finansowe, geolokalizacja),
- odbiorców tych danych, zwłaszcza spoza UE,

- okresy retencji danych (repozytorium dostępne na SGIP SharePoint),
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Grupa SOGECAP jako całość oraz SGIP zidentyfikowała wszystkie procesy przetwarzania danych związane ze swoją działalnością.

Najważniejsze informacje - co musisz wiedzieć

Rejestr czynności przetwarzania zawiera wszystkie informacje związane z operacjami przetwarzania danych osobowych. Informacje te muszą być wpisane do rejestru przed przystąpieniem do przetwarzania i aktualizowane co najmniej raz w roku.

3.1.2. Przetwarzanie danych zgodnie z prawem, w ramach prawnych określonych przez RODO

Aby przetwarzanie danych było zgodne z zasadą legalności, musi być oparte na jednej z sześciu podstaw prawnych przewidzianych w RODO:

- wykonanie umowy z osobą, której dane dotyczą (od propozycji do zakończenia umowy),
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
- realizacja uzasadnionego interesu Administratora lub strony trzeciej, pod warunkiem, że interes ten jest dokładnie określony i udokumentowany, podany do wiadomości osobom, których dane dotyczą i przeważa nad ich interesami, wolnościami i prawami podstawowymi,
- zgoda wyrażona przez osobę, której dane dotyczą,
- ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

W przypadku każdej operacji przetwarzania wybrana podstawa przetwarzania musi być uzasadniona.

Jeżeli podstawą prawną operacji przetwarzania jest uzasadniony interes, kontroler musi ocenić ryzyko i korzyści związane z warunkami, w jakich dane przetwarzanie ma być realizowane.

Analiza ta powinna zostać sformalizowana w dokumencie zwanym oceną prawnie uzasadnionego interesu (LIA).

Najważniejsze informacje - co musisz wiedzieć

Każda operacja przetwarzania danych musi opierać się na jednej z sześciu podstaw prawnych przewidzianych w GDPR. Wybór podstawy prawnej musi być udokumentowany.

3.1.3. Określanie okresów retencji danych zgodnie z celami przetwarzania

Okresy retencji danych są najczęściej określane poprzez odniesienie do zobowiązań prawnych lub regulacyjnych lub zasad dotyczących prawnych okresów przedawnienia. Muszą one być koniecznie określone zgodnie z celem każdej operacji przetwarzania i udokumentowane.

Nie mogą one być nieograniczone. Dział Prawny SGIP opracował, wspólnie z właścicielami operacji przetwarzania, repozytorium okresów retencji danych, dostępne w dedykowanym dokumencie na SGIP SharePoint.

Większość operacji przetwarzania jest ujęta w repozytorium okresów retencji.

W przypadku określonego okresu retencji, który nie pojawia się w repozytorium lub gdy administrator danych potrzebuje zatrzymać dane poza zobowiązaniami prawnymi, wybrany okres retencji musi być uzasadniony i przekazany zespołowi IOD w celu uzyskania walidacji.

Okresy retencji wymienione w repozytorium są okresami stosowanymi do wdrażania mechanizmów technicznych prowadzących do usuwania lub anonimizacji danych osobowych, których wdrażanie nadzoruje inspektor ochrony danych.

Najważniejsze informacje - co musisz wiedzieć

SGIP musi usunąć lub zanonimizować dane osobowe, dla których upłynął okres retencji.

3.1.4. Przeprowadzenie oceny ryzyka dla prywatności każdej z operacji przetwarzania wymienionych w rejestrze

W przypadku, gdy przetwarzanie danych osobowych z dużym prawdopodobieństwem może powodować wysokie ryzyko dla praw i wolności osób fizycznych, administrator danych musi przeprowadzić ocenę skutków dla ochrony danych (PIA).

Zatem w przypadku każdej nowej operacji przetwarzania lub znaczącej aktualizacji operacji przetwarzania właściciel operacji przetwarzania powinien sprawdzić, czy przed wdrożeniem operacji przetwarzania wymagane jest przeprowadzenie PIA.

W tym celu właściciel procesu przetwarzania, przy udziale kierownika projektu, wypełnia dokument zwany PRE PIA, który umożliwia analizę ryzyka dla prywatności związanego z przetwarzaniem danych osobowych, przy wykorzystaniu narzędzia udostępnionego przez Grupę SOGECAP. PRE PIA zawiera dziewięć pytań zdefiniowanych przez Europejską Radę Ochrony Danych, zrzeszającą europejskie organy ochrony danych, na które właściciel procesu udziela odpowiedzi Tak lub Nie. Każda odpowiedź musi być uzasadniona.

PRE PIA jest następnie przesyłana do IOD w celu zatwierdzenia i podjęcia decyzji o przeprowadzeniu lub nieprzeprowadzeniu PIA.

Jeżeli PIA jest wymagana, właściciel procesu przetwarzania wypełnia dokument dostarczony przez Grupę SOGECAP, który składa się z 4 zakładek ponumerowanych od 0 do 3. Powinien on wypełnić zakładki 0 i 1 dotyczące opisu operacji przetwarzania. Bezpieczeństwo IT powinno wypełnić zakładkę 2 i opisać zastosowane środki bezpieczeństwa. Inspektor ochrony danych jest odpowiedzialny za kartę 3 odpowiadającą analizie ryzyka.

Inspektor wydaje opinię na temat przetwarzania i może określić plany działania, jeśli istnieje taka konieczność.

Jeżeli PIA ujawni, że ryzyko rezydualne pozostaje wysokie, IOD wydaje opinię przeciwko wdrożeniu przetwarzania, informuje właściciela przetwarzania i w razie potrzeby eskaluje do odpowiednich osób.

Najważniejsze informacje - co musisz wiedzieć

W przypadku każdej operacji przetwarzania należy przeprowadzić analizę ryzyka w zakresie prywatności: wstępna ocena ryzyka w zakresie prywatności (PRE PIA)

Jeżeli ryzyko jest uważane za wysokie, przeprowadza się szczegółową analizę: PIA.

3.1.5. Regulacja transgranicznego przetwarzania i przekazywania danych poprzez przyjęcie szczególnych środków

Przekazywaniu danych osobowych z organizacji znajdującej się na terenie Europejskiego Obszaru Gospodarczego (EOG) do organizacji znajdującej się w kraju nienależącym do EOG (państwo trzecie) musi towarzyszyć jedno z odpowiednich zabezpieczeń wymienionych w RODO.

Ten obowiązek prawny ma na celu zapewnienie, że przekazywane dane mają zapewniony poziom ochrony odpowiadający poziomowi obowiązującemu w Unii Europejskiej. Przekazywanie danych w ramach EOG nie podlega temu obowiązkowi.

SGIP zapewnia wdrożenie niezbędnych gwarancji w każdym przypadku, gdy operacja przetwarzania wymaga przekazania danych poza EOG. Przepisy te dotyczą przekazywania danych osobowych między podmiotami Grupy Société Générale, a także przekazywania danych przez te same podmioty stronie trzeciej znajdującej się poza EOG (np. dostawcy usług).

W odniesieniu do danych związanych z zasobami ludzkimi: Grupa Société Générale opracowała Wiążące Reguły Korporacyjne i zleciła ich zatwierdzenie w dniu 16/07/2013 przez francuskiego regulatora CNIL. Reguły te same w sobie stanowią odpowiednie zabezpieczenie na mocy RODO. Przekazywanie tych danych może odbywać się bez szczególnych ram umownych, pod warunkiem, że mieści się w jednym z celów określonych w niniejszym dokumencie.

W przypadku danych innych niż dane HR-owe: konieczne jest zapewnienie ram dla wymiany za pośrednictwem gwarancji zalecanych przez Grupę Société Générale.

Najważniejsze informacje - co musisz wiedzieć

Każde przekazanie danych osobowych poza EOG musi być wsparte specjalnymi środkami prawnymi i informatycznymi.

3.2. Dostarczanie osobom, których dane dotyczą, wszystkich informacji związanych z przetwarzaniem ich danych osobowych

RODO wyraża obowiązki w zakresie informowania osób, których dane osobowe są przetwarzane przez SGIP. Osobami tymi mogą być pracownicy, klienci, potencjalni klienci lub jakiekolwiek inne osoby fizyczne będące osobami trzecimi.

Osoby, których dane osobowe są przetwarzane, muszą zostać poinformowane o:

- warunkach wykorzystania ich danych: celu, podstawie prawnej,

- odbiorcach ich danych,

- okresie retencji danych,

- przysługujących im prawach,

- możliwości wniesienia skargi do właściwego organu ochrony danych.

Informacje te muszą być dostarczone przez administratora danych w momencie zbierania danych. Są one dostarczane głównie poprzez dokumentację umowną lub stronę internetową. Mogą być również przekazane przez podmiot przetwarzający dane na podstawie umowy.

Istnieją 2 rodzaje gromadzenia danych:

- zbieranie bezpośrednie, gdzie dane zbierane są bezpośrednio od osób fizycznych (np. formularz, subskrypcja itp.),

- gromadzenie pośrednie, kiedy dane są zbierane od strony trzeciej (np. dane uzyskiwane od partnera, brokera, służb publicznych).

SGIP komunikuje się w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny. W szczególności zapewnia, że używa terminów, które są jasne i zrozumiałe dla osób, którym informacje są przekazywane.

W przypadku pośredniego zbierania danych, SGIP informuje osoby, których dane dotyczą, o kategoriach przetwarzanych danych i źródle ich pochodzenia, jeżeli nie posiadają one tych informacji w momencie ich wykorzystania (np. informacje o uposażonych w chwili śmierci w ubezpieczeniach na życie).

Najważniejsze informacje - co musisz wiedzieć

Za każdym razem, gdy SGIP gromadzi dane osobowe, musi poinformować osoby, których te dane dotyczą, o sposobie ich wykorzystania oraz o przysługujących im prawach.

3.3. Reagowanie na wnioski o wykonanie praw składane przez osoby, których dane dotyczą

Podmiotami danych, których dotyczy przetwarzanie danych osobowych, mogą być klienci, pracownicy, usługodawcy, potencjalni klienci, osoby kontaktowe, dostawcy, dyrektorzy firm itp.

Podmioty te mają prawo:

- dostępu do swoich danych,
- sprostowania błędnych danych,
- do usunięcia danych ("prawo do bycia zapomnianym"),
- do przenoszenia danych,
- sprzeciwu wobec przetwarzania,
- ograniczenia przetwarzania swoich danych,
- do niepodlegania czysto zautomatyzowanym decyzjom, w tym profilowaniu.

Każde z tych praw ma określony zakres zastosowania, co niekiedy może ograniczać lub opóźniać ich realizację.

I tak, klient nie może żądać usunięcia swoich danych bezpośrednio po rozwiązaniu umowy, nie może też żądać sprostowania danych innej osoby.

Nieprzekraczalny termin na udzielenie odpowiedzi na wnioski o wykonanie praw wynosi 30 dni od otrzymania wniosku, ale w przypadku złożonych wniosków może on zostać przedłużony o 60 dni. Inspektor ochrony danych prowadzi rejestr wniosków dotyczących praw RODO.

Najważniejsze informacje - co musisz wiedzieć

SGIP musi odpowiedzieć na wnioski o wykonanie praw w ciągu 30 dni

3.4. Wdrażanie środków niezbędnych do zapewnienia bezpieczeństwa danych osobowych

3.4.1. Minimalizacja wykorzystania danych osobowych - zasada minimalizacji

Zasada minimalizacji stanowi, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, dla których są przetwarzane.

Przestrzeganie zasady minimalizacji oznacza przetwarzanie tylko tych danych osobowych, które są niezbędne do osiągnięcia celu, zarówno pod względem czasu trwania przetwarzania, jak i ilości przetwarzanych danych lub liczby osób mających dostęp do danych osobowych.

W związku z tym SGIP nie może wykorzystywać nazwisk/imion/daty urodzenia, jeżeli zamiast nich może wykorzystać identyfikator komputerowy. Podobnie liczba osób, które mogą uzyskać dostęp do danych, musi być ograniczona, tylko do tych, których zadanie tego wymaga, i tylko na czas niezbędny do przetwarzania danych.

SGIP zobowiązuje się do realizacji zasady minimalizacji.

Najważniejsze informacje - co musisz wiedzieć

Przetwarzane dane osobowe oraz liczba osób mających dostęp do tych PD powinny być zawsze ograniczone do niezbędnego minimum.

3.4.2. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Zgodność z zasadą ochrony prywatności w fazie projektowania oznacza uwzględnienie, już na etapie opracowywania i projektowania wszelkich nowych produktów, usług lub aplikacji wiążących się z przetwarzaniem danych osobowych, wszystkich zasad mających zastosowanie w RODO, w szczególności środków bezpieczeństwa i przyjęcia mechanizmów chroniących prawa osób, których dane dotyczą.

Przestrzeganie zasady domyślnej ochrony danych wymaga stosowania najwyższego poziomu ochrony gromadzonych i przetwarzanych danych osobowych, w szczególności ograniczenia przetwarzania danych osobowych do tego, co jest niezbędne do osiągnięcia celu.

SGIP zobowiązuje się do wdrożenia zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych, aby ograniczyć przetwarzanie danych do tego, co jest ściśle niezbędne do osiągnięcia danego celu.

3.4.3. Wdrażanie odpowiednich środków technicznych i organizacyjnych

SGIP wdraża odpowiednie środki techniczne i organizacyjne w celu zagwarantowania poziomu bezpieczeństwa dostosowanego do ryzyka, zgodnie z polityką bezpieczeństwa informacji i bezpieczeństwa systemów informacyjnych SGIP. Środki te muszą zapewnić odpowiednie bezpieczeństwo i poufność danych, w szczególności uniemożliwić ich:

- przekazanie (ujawnianie lub udostępnianie) nieuprawnionym osobom trzecim,
- modyfikację (zmiany itp.),
- uszkodzenie (przypadkowe lub bezprawne zniszczenie, utrata itp.).

Te środki i sposoby są określane przez kierowników ds. bezpieczeństwa systemów informacyjnych. Są one udokumentowane w regularnie aktualizowanych dokumentach referencyjnych.

W związku z tym SGIP uwzględnia ochronę danych osobowych już w fazie projektowania umów, produktów i systemów informatycznych. Zapewnia, że bezpieczeństwo danych osobowych jest zagwarantowane podczas wszystkich operacji, dla których są one gromadzone, przetwarzane i przechowywane, aż do ich usunięcia lub anonimizacji.

Najważniejsze informacje - co musisz wiedzieć

Podmioty przetwarzające muszą zapewnić, że aplikacje, z których korzystają, posiadają środki bezpieczeństwa odpowiednie do wrażliwości zarządzanych danych lub że wdrożone procesy pozwalają na przetwarzanie danych osobowych z wymaganym poziomem bezpieczeństwa.

3.4.4. Zapobieganie naruszeniom ochrony danych osobowych i zarządzanie nimi

Naruszenie ochrony danych osobowych to zdarzenie związane z bezpieczeństwem, umyślne lub nieumyślne, w wyniku którego poufność, integralność lub dostępność danych osobowych zostaje zagrożona.

SGIP zbudował korpus normatywny do zarządzania naruszeniami ochrony danych osobowych, który identyfikuje interesariuszy zaangażowanych w postępowanie w przypadku naruszenia i ich role, dostępny na SGIP SharePoint.

Jeśli pracownik SGIP znajdzie się w sytuacji, w której:

- może uzyskać dostęp do danych osobowych, zmienić je lub usunąć,

- i jeśli uważa, że nie powinien mieć takiej możliwości,

zawiadamia bez zbędnej zwłoki inspektora ochrony danych.

Każdy incydent dotyczący przetwarzania danych osobowych musi być niezwłocznie zgłoszony inspektorowi ochrony danych, który analizuje incydent i ocenia poziom ryzyka.

Inspektor wydaje zalecenie kierownikom działów, których dotyczy incydent, dotyczące potrzeby powiadomienia właściwego organu nadzoru lub nawet osób, których dane dotyczą. W razie potrzeby powiadomienie właściwego organu nadzoru jest dokonywane jak najszybciej i nie później niż 72 godziny po uzyskaniu informacji o naruszeniu.

Zaangażowani właściciele danych (naruszenie danych osobowych w ich obrębie), wdrażają niezbędne działania naprawcze tak szybko, jak to możliwe i są odpowiedzialni za powiadomienie osób, których dane dotyczą, w razie potrzeby, wspólnie z inspektorem ochrony danych.

ASSU DPO musi zostać poinformowany przed jakimkolwiek powiadomieniem organu nadzoru przez jedną ze spółek zależnych lub oddziałów znajdujących się na terytorium europejskim i działa jako łącznik z IOD Grupy SOCIETE GENERALE.

W przypadku naruszenia mającego wpływ na kilku administratorów danych w Grupie SOGECAP, koordynacja analizy naruszenia i poziomu jego powagi jest obowiązkiem ASSU DPO, który zapewnia, że odpowiedzi udzielone różnym Organom Ochrony są jednolite i skoordynowane.

Po zgłoszeniu incydentu do organu ochrony danych, jest on przedstawiany "Komitetowi ds. incydentów zgodności" Grupy Société Générale.

Najważniejsze informacje - co musisz wiedzieć

Naruszenia ochrony danych osobowych powinny być natychmiast zgłaszane do IOD.

Wszelkie zgłoszenia do polskiego organu ochrony danych muszą być dokonane w ciągu 72 godzin od wykrycia incydentu.

3.5. Zarządzanie relacjami z dostawcami usług i podmiotami przetwarzającymi

SGIP posiada ramy umowne dla relacji z partnerami przetwarzającymi dane osobowe. Na bieżąco aktualizuje umowy ze swoimi partnerami i określa w nich role i obowiązki partnerów.

Systematycznie przeprowadzana jest analiza w celu ustalenia, czy SGIP jest "administratorem danych", "współadministratorem danych", "odrębnym administratorem danych" lub "podmiotem przetwarzającym".

- Administrator jasno i precyzyjnie określa cele i środki każdej z operacji przetwarzania danych osobowych, które realizuje. Wydaje instrukcje swojemu procesorowi (swoim procesorom) w zakresie, między innymi, okresu retencji i usuwania danych osobowych. Ocenia poziom bezpieczeństwa przetwarzania tych danych przed zawarciem umowy.

- W przypadku, gdy SGIP jest "Podmiotem przetwarzającym", gromadzi i przetwarza dane osobowe w ścisłej zgodności z obowiązującymi przepisami lub umową oraz zgodnie z instrukcjami przekazanymi mu przez administratora danych.

- Jeżeli cele i środki operacji przetwarzania są określane wspólnie przez dwa lub więcej podmiotów działających jako administratorzy, mogą oni być uznani za współadministratorów tej operacji przetwarzania. Powinni oni wówczas określić, w sposób przejrzysty i na piśmie, swoje odpowiednie role i obowiązki w odniesieniu do operacji przetwarzania.

Grupa SOGECAP zapewnia narzędzie, które pomaga liniom biznesowym w określeniu linii relacji z partnerem.

Załączniki

Załącznik 1 Intranet link

The GDPR Intranet of the SOGECAP Group is accessible at https://sg-insurance.safe.socgen/fr/rgpd

Załącznik 2 Dokumenty

	Nazwa dokumentu	Status
1	Personal data protection policy	Zwalidowany
2	Personal data breach management procedure	Zwalidowany
3	Non-employee rights request management procedure	Zwalidowany
4	Employee rights request management procedure	Zwalidowany
5	Non-employee rights request management standard operating procedure	Zwalidowany
6	Employee rights request management standard operating procedure	Zwalidowany
7	PIA tool with user guide	Zwalidowany
8	Pre-PIA tool with user guide	Zwalidowany

SOCIETE GENERALE
Insurance