Załącznik nr 14

Polityka bezpieczeństwa w zakresie monitoringu wizyjnego oraz monitoringu narzędzi powierzanych pracownikom

§ 1

Zasady wprowadzania monitoringu wizyjnego i monitoringu narzędzi

1. Monitoring wizyjny, jak również monitoring narzędzi powierzanych pracownikom, np. dostęp do Internetu, wykorzystanie poczty elektronicznej, wykorzystanie komputera w szczególności oprogramowania, itp. może powodować naruszenie praw i wolności osób podlegających monitorowaniu, a także osób trzecich objętych zapisami monitoringu.
2. Monitoring narzędzi powierzanych pracownikom, np. dostęp do Internetu, wykorzystanie poczty elektronicznej, wykorzystanie komputera w szczególności oprogramowania, może być wdrażany i stosowany w Banku wyłącznie w przypadkach dopuszczalnych przez prawo oraz na zasadach niniejszej Polityki.

§ 2

Rozliczalność

1. Bank realizuje wszystkie prawa jakie przysługują osobie, której dane osobowe są przetwarzane w związku z monitoringiem, w szczególności na zasadach wynikających z ogólnych regulacji dotyczących przetwarzania danych osobowych.
2. Podstawą wdrożenia i stosowania monitoringu wizyjnego oraz monitoringu narzędzi powierzanych pracownikom może być uzasadniony prawnie interes realizowany przez Bank lub przez stronę trzecią, tzn. art. 6 ust. 1 lit. f RODO - istnienie tego interesu musi być poddawane analizie w celu wykazania jego faktycznego występowania.
3. Niezbędność przetwarzania w zakresie monitoringu podlega analizie na zasadach art. 5 ust. 1 lit. c RODO, tzn. przestrzegania zasady minimalizacji danych obligującej Bank do przetwarzania jedynie tych danych osobowych, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których dane są przetwarzane.
4. W celu zapewnienia rozliczalności zgodnie z art. 5 ust. 2 RODO:
   1) każdorazowe wprowadzenie monitoringu, zmiana zakresu jego stosowania lub zasad stosowania podlega udokumentowanej analizie zgodności z przepisami prawa oraz obowiązującymi wytycznymi UODO (Urząd Ochrony Danych Osobowych) lub

EROD (Europejska Rada Ochrony Danych), w tym analizie wykazującej istnienie prawnego interesu Banku lub strony trzeciej, a także niezbędności przetwarzania;

2) przetwarzanie danych w ramach monitoringu podlega udokumentowaniu w postaci gromadzenia odpowiednich zapisów w postaci dokumentów lub zapisów w systemach informatycznych, w szczególności dotyczy to:
   a) nadawania uprawnień do przetwarzania danych w ramach monitoringu - może odbywać się to poprzez zastosowanie ogólnej procedury związanej z nadawaniem uprawnień do przetwarzania danych osobowych;
   b) udokumentowania dostępu pracowników Banku lub podmiotów przetwarzających (np. pracowników serwisu) do nagrań lub zapisów monitoringu – np. poprzez rejestrację dostępu do systemów monitoringu w odpowiedniej ewidencji lub logach;
   c) udostępniania nagrań lub zapisów monitoringu uprawnionym podmiotom trzecim –np. poprzez rejestrację udostępnienia nagrań lub informacji do systemów monitoringu w odpowiedniej ewidencji;
   d) dokumentowania usuwania nagrań lub zapisów, zarówno w przypadku czynności inicjowanych przez pracowników lub poprzez działanie mechanizmu automatycznego.

5. Odpowiednie dokumenty analiz, ewidencje oraz rejestry prowadzą lub administrują nimi:
   1) Pracownik Bezpieczeństwa Informacji w zakresie:
      a) analiz wykazujących istnienie prawnego interesu Banku lub strony trzeciej, a także niezbędności przetwarzania;
      b) rejestrów i ewidencji uprawnień do przetwarzania danych w ramach monitoringu - może odbywać się to poprzez zastosowanie ogólnej procedury związanej z nadawaniem uprawnień do przetwarzania danych osobowych;
      c) rejestracji dostępu pracowników Banku lub podmiotów przetwarzających (np. pracowników serwisu) do nagrań lub zapisów;
      a) rejestracji udostępniania nagrań lub zapisów monitoringu uprawnionym podmiotom trzecim;
      b) dokumentowania usuwania nagrań lub zapisów.

§ 3

Dozwolony zakres wprowadzania monitoringu wizyjnego

1. Bank może wprowadzić szczególny nadzór nad terenem Banku lub terenem wokół Banku w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring), jeżeli

jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji usług lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Bank na szkodę.

2. Monitoring wizyjny nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni lub pomieszczeń udostępnianych zakładowej organizacji związkowej, chyba, że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego w ust. 2 i nie naruszy to godności oraz innych dóbr osobistych pracownika, a także zasady wolności i niezależności związków zawodowych, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób.
3. Monitoring wizyjny powinien być ograniczony do lokali, obiektów czy pomieszczeń, które znajdują się w posiadaniu Banku. Kamery lub inne urządzenia rejestrujące obraz nie powinny obejmować swym zakresem np. przestrzeni publicznych czy innych sąsiadujących terenów. W przypadku niemożności uniknięcie takich sytuacji, np. z uwagi na techniczne uwarunkowania należy wdrożyć blokowanie pola rejestracji obrazu lub pikselizację obrazu w części ukazującej sąsiadujące obszary.

§ 4

Monitorowanie pracowników

1. Cele, zakres oraz sposób zastosowania monitoringu wizyjnego oraz monitoringu stosowanych narzędzi ustala się w **Regulaminie pracy** obowiązującym w Banku.
2. Bank informuje pracowników o wprowadzeniu monitoringu wizyjnego oraz monitoringu powierzanych pracownikom narzędzi, poprzez dostarczenie im informacji na piśmie, nie później niż 2 tygodnie przed jego uruchomieniem.
3. Bank przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje, o których mowa w ust 1.
4. W przypadku wprowadzenia monitoringu wizyjnego Bank oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem.
5. Bank może wprowadzić kontrolę wykorzystania narzędzi powierzonych pracownikowi np. służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej) lub innych narzędzi, w tym np. dostępu do Internetu, wykorzystania komputera, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej

pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy.

6. Monitoring poczty elektronicznej lub innych narzędzi powierzonych pracownikowi nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.

§ 5

Okres przechowywania danych

1. Nagrania obrazu pochodzące z monitoringu wizyjnego Bank przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres nieprzekraczający 3 miesięcy od dnia nagrania.
2. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin określony w ust. 1 ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.
3. Zapisy monitoringu stosowania narzędzi są przechowywane przez okres wynikający z prawnie uzasadnionego interesu Banku, tzn. w okresie do terminu przedawnienia roszczeń Banku wobec pracownika, tzn. rok po zakończeniu stosunku pracy.
4. Po upływie okresów, o których mowa w ust. 1 do ust. 3 , uzyskane w wyniku monitoringu nagrania obrazu lub zapisy monitoringu wykorzystania narzędzi zawierające dane osobowe, podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.
5. Zalecanym rozwiązaniem jest wprowadzenie mechanizmu automatycznego usuwania zapisów z monitoringu.

§ 6

Obowiązek informacyjny

1. Bank przetwarzając dane osobowe uzyskane w drodze monitoringu wizyjnego lub monitoringu wykorzystania narzędzi, zobligowany jest do spełnienia obowiązku informacyjnego zgodnie z art. 13, a także art. 12 RODO.
2. Pierwszy etap wykonania obowiązku informacyjnego:
   1) polega na umieszczeniu w widocznym miejscu „znaku ostrzegawczego” – np. piktogramu oraz podstawowych informacji wskazujących na obszary objęte monitoringiem, cele przetwarzania danych, najważniejsze skutki przetwarzania danych, przekazywanie danych podmiotom trzecim (jeśli są przekazywane), okresy retencji, tożsamość administratora danych oraz dane kontaktowe inspektora ochrony

danych. Bank powinien ponadto określić miejsce, w którym dana osoba będzie mogła zapoznać się w klauzulą informacyjną „w pełnej wersji”;

2) „Znak ostrzegawczy” powinien znajdować się przed pomieszczeniami / obiektami objętymi monitoringiem wizyjnym, tak aby umożliwić danej osobie podjęcie świadomej decyzji co do tego, czy chce wejść na monitorowany teren.
3) Umieszczenie przed wejściem do obiektu monitorowanego ikony symbolizującej kamerę i opatrzonej hasłem ostrzegawczym jest sprzeczne z RODO. Na pierwszym etapie osoba, której dane osobowe miałyby podlegać przetwarzaniu, powinna uzyskać zestaw najważniejszych informacji określonych w art. 13 RODO.

3. Drugi etapu spełnienia obowiązku informacyjnego:
   1) obejmuje umieszczenie w miejscu łatwo dostępnym kompletnej klauzuli informacyjnej zgodnie z wymaganiami art. 13 RODO;
   2) klauzula ta powinna być dostępna co najmniej w formie tradycyjnej, np. poprzez przygotowanie jej w wersji papierowej do wglądu w placówce Banku czy w formie informacji umieszczonej na tablicy ogłoszeń w miejscu dobrze widocznym;
   3) dobrą praktyką jest również zapewnienie dodatkowo innych możliwości zapoznania się z klauzulą, np. poprzez zamieszczenie linku do strony internetowej.
4. Obowiązki informacyjne wobec pracowników obejmują dodatkowo zasady wymienione w § 4, a także w razie potrzeby odpowiednie informacje lub oświadczenia zawarte w regulacjach kadrowych.
5. Wzory obowiązków informacyjnych są zawarte w Załączniku nr 14A, !4B, 14C.

§ 7

Kontrola dostępu do zarejestrowanych nagrań lub zapisów monitoringu

1. Dostęp do zarejestrowanych nagrań monitoringu wizyjnego lub zapisów monitoringu wykorzystania narzędzi (np. poczty elektronicznej, logów systemów) mają wyłącznie upoważnione osoby, powinny one korzystać z tego dostępu wyłącznie w uzasadnionych przypadkach, wynikających z celu przetwarzania danych.
2. Bank stosuje środki kontroli dostępu do nagrań monitoringu wizyjnego lub zapisów monitoringu wykorzystania narzędzi, obejmuje to kontrolę dostępu logicznego (tam gdzie to możliwe) np. w postaci odpowiednich haseł dostępu do systemów monitoringu, a także kontrolę fizyczną w postaci ograniczenia dostępu do pomieszczeń lub urządzeń (np. odpowiednia, zamknięta szafa lub pomieszczenie zawierająca urządzenia) do osób upoważnionych.

3. Dostęp do systemów monitoringu jest każdorazowo odnotowywany w odpowiedniej ewidencji, która może mieć postać papierową lub elektroniczną (log w systemie).

§ 8

Udostępnianie zarejestrowanych nagrań lub zapisów monitoringu

1. Udostępnianie nagrań monitoringu wizyjnego lub zapisów monitoringu wykorzystania narzędzi jest możliwe w przypadkach wynikających z przepisów prawa lub uzasadnionego prawnie interesu realizowanego przez Bank lub przez stronę trzecią.
2. Udostępnienia nagrania lub zapisu monitoringu może nastąpić z inicjatywy Banku, w celu realizacji uzasadnionego prawnie interesu Banku lub na wniosek lub żądanie uprawnionego organu (np. Policja) lub osoby trzeciej, wynikającego z obowiązujących przepisów prawa.
3. Decyzję o udostępnieniu nagrania lub zapisu monitoringu podejmuje osoba upoważniona przez Zarząd, np. członek Zarządu lub odpowiedni pracownik.
4. W przypadku wątpliwości związanych z możliwością udostępnienia danych osobowych zawartych w nagraniach monitoringu wizyjnego lub zapisów monitoringu wykorzystania narzędzi należy uzyskać opinię prawną.
5. Udostępnianie nagrań monitoringu wizyjnego lub zapisów jest każdorazowo odnotowywane w odpowiedniej ewidencji, która może mieć postać papierową lub elektroniczną.