**JAK OCENIĆ RYZYKO NARUSZENIA DANYCH OSOBOWYCH**

Dla wszystkich procesów przetwarzania danych osobowych należy określić poziom ryzyka związanego z przetwarzaniem danych osobowych i wdrożyć odpowiednie środki zabezpieczenia danych. Podejście oparte na ryzyku wymaga ciągłego monitorowania poziomu ryzyka związanego z przetwarzaniem danych osobowych. Nie jest więc wystarczającym jednorazowe dla danego procesu określenie poziomu ryzyka i zastosowanie środków zabezpieczenia danych – poziom ryzyka powinien być monitorowany ciągle w ramach trwających procesów przetwarzania danych.

Przykładowe elementy wpływające na ocenę ryzyka naruszenia danych osobowych:

|  |  |
| --- | --- |
| **RYZYKO WZRASTA** | **RYZYKO MALEJE** |
| **Ilość użytkowników** | |
| Do przetwarzania danych osobowych zaangażowana jest znaczna ilość użytkowników. | Administrator sam przetwarza dane osobowe, bez pomocy jakiegokolwiek użytkownika. |
| **Komentarz**: Użytkownicy tj. pracownicy, zleceniobiorcy, praktykanci, stażyści zawsze są uznawani za najsłabsze ogniwo jeżeli chodzi o ochronę danych osobowych. Im większa ilość użytkowników tym większe ryzyko naruszenia danych osobowych. Oczywiście należy pamiętać o upoważnieniu do przetwarzania danych osobowych – brak upoważnienia dla użytkownika nie tylko zwiększa ryzyko naruszenia danych osobowych, ale stanowi poważne naruszenie ze strony administratora danych. | |
| **Szkolenie użytkowników** | |
| Użytkownicy nie ukończyli szkolenia z zakresu ochrony danych osobowych. | Użytkownicy ukończyli szkolenie w zakresie ochrony danych osobowych. |
| **Komentarz**: Przeszkolony użytkownik z pewnością będzie miał większą świadomość ochrony danych osobowych w firmie. Ukończenie krótkiego kursu z pewnością obniża ryzyko naruszenia danych osobowych, niż w przypadku braku jakichkolwiek informacji na temat legalnego i bezpiecznego przetwarzania danych osobowych. | |
| **Dostęp do sieci internet** | |
| Dane osobowe są przetwarzane za pośrednictwem systemu komputerowego podłączonego do sieci internet | Dane osobowe są przetwarzane za pośrednictwem tradycyjnej formy papierowej. |
| **Komentarz**: Podłączenie do sieci internet należy uznać za element podwyższający ryzyko naruszenia danych osobowych, wynika to z możliwości np. instalacji wirusa blokującego lub wykradającego dane z systemu informatycznego. | |
| **Antywirus** | |
| Brak antywirusa lub zapory ogniowej na stanowisku komputerowym. | Instalacja antywirusa na stanowisku komputerowym. |
| **Komentarz**: Dla stanowisk podłączonych do sieci internet absolutny obowiązek stanowi posiadanie programu antywirusowego – jego brak może uznać za rażącą niedbałość administratora. Posiadanie programy dotyczy także stanowisk nie podłączonych do sieci. | |
| **Zabezpieczenia fizyczne** | |
| Brak zabezpieczeń fizycznych pomieszczeń w których są przetwarzane dane osobowe | Pomieszczenia fizyczne w których są przetwarzane dane osobowe posiadają zabezpieczenia uniemożliwiające dostęp osób postronnych. |
| **Komentarz**: RODO wymaga zastosowania środków ochrony danych osobowych adekwatnych do poziomu ryzyka naruszenia. Co to oznacza? Nie ma obowiązku posiadania krat w oknach, niszczarek czy sejfu na dokumenty. Oczywiście tego rodzaju zabezpieczenia powodują, że ryzyko naruszenia danych osobowych znacząco maleje, ale równie dobrze można chronić dane w zamykanych szafach, do których dostęp mają wyłącznie upoważnieni użytkownicy. To jakie zabezpieczenia zastosuje administrator danych zależy tylko od niego. Najważniejszym elementem jest dostosowanie środków ochrony do rodzaju przetwarzanych danych (np. dane wrażliwe powinny być lepiej chronione) oraz ilości danych. | |
| **Powierzenie danych osobowych** | |
| Podmiot w celu wykonywania działalności przekazuje dane osobowe innym przedsiębiorcom bez podpisanych umów powierzenia danych osobowych. | Podmiot w celu wykonywania działalności przekazuje dane osobowe innym przedsiębiorcom – łączy ich umowa powierzenia danych osobowych. |
| **Komentarz**: W celu wykonywania działalności gospodarczej konieczne jest korzystanie z usług innych przedsiębiorców jednak zgodnie z RODO należy korzystać z usług tylko takich przedsiębiorców, którzy dają rękojmię poprawnej ochrony danych osobowych, a tego rodzaju oświadczenie (deklaracja) powinna wynikać z umowy powierzenia danych osobowych. | |
| **Czas przetwarzania danych osobowych** | |
| Dane osobowe będą przetwarzane przez okres 50 lat np. dokumentacja osobowa pracownika od dnia zakończenia pracy u pracodawcy - zgodnie z art. 51u ustawy o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2016 r., poz. 1506) | Dane osobowe będą przetwarzane przez okres 5 lat np. dowody księgowe zgodnie z art. 74 ust. 2 pkt 8 ustawy o rachunkowości z 29 września 1994 r. (Dz. U. 2018. 395) |
| **Komentarz**: Okres w jakim administrator przetwarza dane osobowe również ma wpływ na ocenę ryzyka. Ryzyko zawsze będzie wzrastać jeżeli okres przechowywania danych jest długi, a maleć jeżeli jest krótki. Wynika to z faktu, iż w dłuższym okresie przetwarzania (archiwizacji) danych istnieje większe prawdopodobieństwo naruszenia danych. | |

**MONITORING**

Ogólne zestawienie mocnych i słabych stron naszego przedsiębiorstwa w zakresie ochrony danych osobowych umożliwia ocenę poziomu ryzyka naruszenia danych osobowych. Warto jednak pamiętać o monitorowaniu ryzyka np. konieczna jest aktualizacja programu antywirusowego w celu uniknięcia najnowszych zagrożeń krążących po sieci – brak aktualizacji powoduje wzrost ryzyka, instalacja aktualizacji powoduje obniżenie ryzyka.

**Przykładowa analiza ryzyka**

Niniejszy dokument został przygotowany w toku procesu wdrożenia ochrony danych osobowych w ramach działalności gospodarczej prowadzonej przez:

|  |  |
| --- | --- |
| **Firma:** | Legalniewsieci.pl Sp. z o.o. |
| **Adres siedziby:** | ul. Młyńska 23,  40-098 Katowice |
| **NIP:** | 6342902737 |
| **REGON:** | 368023160 |
| **Liczba użytkowników** (*tj. liczba osób w przetwarzających dane osobowe w przedsiębiorstwie*) | 3 użytkowników |

Administrator danych osobowych przeprowadził analizę ryzyka, której celem była ocena zagrożeń dla poprawnego i bezpiecznego przetwarzania danych osobowych oraz wybór   
i wdrożenie środków zmniejszających prawdopodobieństwo wystąpienia tychże zagrożeń.

Elementy, które mają znaczenie na ocenę ryzyka związanego z przetwarzaniem danych osobowych to:

1. administrator wykonuje działalność gospodarczą w jednej lokalizacji,
2. w tej lokalizacji dochodzi do przetwarzania danych osobowych,
3. administrator zatrudnia mniej niż 10 pracowników,
4. administrator powierza przetwarzanie danych osobowych podmiotom o uznanej renomie i cieszących się reputacją w środowisku branżowym,
5. administrator wykorzystuje do przetwarzania danych osobowych systemy informatyczne, instalowane na dysku komputera, a systemy te należą do powszechnie wykorzystywanych przez przedsiębiorców w ramach prowadzonych działalności gospodarczych,
6. administrator wykorzystuje do przetwarzania danych osobowych systemy informatyczne funkcjonujące w modelu dostępu on-line, a systemy te należą do powszechnie wykorzystywanych przez przedsiębiorców w ramach prowadzonych działalności gospodarczych,
7. administrator wykorzystuje przy przetwarzaniu danych komputery,
8. administrator przetwarza dane w formie elektronicznej,
9. administrator nie przetwarza danych osobowych na dużą skalę,
10. administrator przetwarza dane osobowe wrażliwe, ale nie na dużą skalę.

**Opis oraz identyfikacja wymagań prawnych i techniczno-organizacyjnych**

Wszystkie czynności przetwarzania danych osobowych zostały skatalogowane   
w rejestrze czynności przetwarzania danych osobowych. Przygotowanie rejestru pozwoliło administratorowi stwierdzić, że dane osobowe zbierane są zgodnie z prawem, w tym z adekwatnością celu i proporcjonalnością. Administrator zbiera tylko takie dane, które są niezbędne do realizacji określonych celów, nie gromadząc przy tym danych nadmiarowych. Ponadto, dane przetwarzane są przez uzasadniony określonymi celami czas.

Administrator realizuje w stosunku do osób, których dane przetwarza obowiązek informacyjny, dostarczając tym osobom informacji, o których mowa w art. 13 RODO. Ponadto, administrator zapewnia tym osobom możliwość realizacji ich uprawnień, o których mowa w art. 16 – 21 RODO.

**Przewidywane ryzyka**

W związku ze zidentyfikowanymi czynności przetwarzania danych osobowych, administrator dostrzega następujące potencjalne ryzyka:

* niewłaściwe postępowanie z danymi osobowymi przez osoby upoważnione do przetwarzania danych,
* uzyskanie dostępu do danych w systemach informatycznych przez osoby nieuprawnione,
* włamanie do systemu informatycznego, w którym dane są przetwarzane,
* kradzież sprzętu wykorzystywanego do przetwarzania danych osobowych, na którym dane są przechowywane,
* nieuprawnione wykorzystanie danych powierzonych do przetwarzania przez procesorów,
* przypadkowe usunięcie danych osobowych z systemów informatycznych,
* awaria systemów informatycznych powodująca czasową niedostępność danych,
* awaria systemów informatycznych skutkująca usunięciem danych,
* uzyskanie dostępu do danych przekazywanych drogą teletransmisji przez osoby do tego nieuprawnione.

**Minimalizacja ryzyka**

W celu zminimalizowania ryzyka związanego z przetwarzaniem danych osobowych administrator wdrożył środki organizacyjne i techniczne wskazane w polityce ochrony danych osobowych. Na potrzeby analizy ryzyka, administrator przyporządkował te środki do poszczególnych rodzajów ryzyka, co znajduje odzwierciedlenie poniżej.

Niewłaściwe postępowanie z danymi osobowymi przez osoby upoważnione do przetwarzania danych:

* przeszkolenie osób upoważnionych do przetwarzania danych osobowych z zakresu ochrony danych osobowych,
* zobowiązanie osób przetwarzających dane do zachowania ich w tajemnicy,
* zaznajomienie osób przetwarzających dane ze wszelkimi politykami związanymi   
  z postępowaniem z danymi osobowymi,
* zastosowanie systemowych środków pozwalających na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

Uzyskanie dostępu do danych w systemach informatycznych przez osoby nieuprawnione:

* dostęp do systemów informatycznych wymaga zalogowania z wykorzystaniem nazwy użytkownika oraz hasła, a każda osoba przetwarzająca dane posiada oddzielną nazwę użytkownika oraz hasło,
* dostęp do systemów informatycznych wymaga użycia szyfrującego klucza sprzętowego (licencyjnego),
* silne hasło składające się co najmniej z 8 znaków, w tym z liter i cyfr,
* korzystanie ze sprawdzonych i cieszących się renomą systemów informatycznych,
* zainstalowanie wygaszaczy ekranów na stanowiskach, na których przetwarzane są dane osobowe,
* zastosowanie mechanizmu automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Włamanie do systemów informatycznych, w których przetwarzane są dane:

* korzystanie ze sprawdzonych i cieszących się renomą systemów informatycznych   
  w celu posiadania pewności, że infrastruktura techniczna systemów jest należycie zabezpieczona,
* korzystanie z oprogramowania antywirusowego i Firewall,
* zastosowanie systemowego mechanizmu wymuszającego okresową zmianę haseł,
* zastosowanie środków ochrony przed szkodliwym oprogramowaniem.

Kradzież sprzętu wykorzystywanego do przetwarzania danych osobowych, na którym dane są przechowywane:

* szyfrowanie dysków, na których znajdują się dane osobowe,
* zabezpieczenie dostępu do systemu operacyjnego sprzętu za pomocą nazwy użytkownika oraz hasła,
* dostęp do zbioru danych osobowych wymaga użycia szyfrującego klucza sprzętowego (licencyjnego),
* szyfrowanie zbioru bazy danych, w której przechowywane są dane osobowe,
* silne hasło składające się co najmniej z 8 znaków, w tym z liter i cyfr.

Nieuprawnione wykorzystanie danych powierzonych do przetwarzania przez procesorów:

* zawarcie umów powierzenia odpowiedniej treści,
* odpowiedni dobór procesorów spośród podmiotów o uznanej reputacji,
* wdrożenie środków uniemożliwiających wykonywanie nieautoryzowanych kopii danych przetwarzanych przy użyciu systemów informatycznych.

Przypadkowe usunięcie danych osobowych z systemów informatycznych:

* wykonywanie kopii zapasowych,
* przeszkolenie osób przetwarzających dane z zakresu posługiwania się systemami informatycznymi.

Awarie systemów informatycznych:

* wykonywanie kopii zapasowych,
* odpowiedni dobór systemów informatycznych spośród tych cieszących się uznaniem.

Uzyskanie dostępu do danych przekazywanych drogą teletransmisji przez osoby do tego nieuprawnione:

* korzystanie z bezpiecznego połączenia SSL,
* zastosowanie środków kryptograficznej ochrony danych,
* zabezpieczenie dostępu do danych za pomocą mechanizmów uwierzytelnienia.

**Wnioski**

Biorąc pod uwagę, że administrator danych osobowych:

1. prowadzi działalność gospodarczą, która nie powoduje szczególnego zagrożenia związanego z ochroną danych osobowych,
2. przetwarza dane osobowe wrażliwe, ale nie na dużą skalę,
3. nie posiada rozbudowanej struktury organizacyjnej,
4. korzysta z podstawowych, powszechnie stosowanych systemów informatycznych służących do przetwarzania danych osobowych, których dostawcy gwarantują odpowiedni poziom bezpieczeństwa danych osobowych w nim przetwarzanych,
5. wdrożył niezbędne środki ochrony danych osobowych w celu należytego zabezpieczenia danych osobowych i ograniczenia do minimum ryzyka zaistnienia incydentu naruszenia ochrony danych osobowych,

**Podsumowanie**

Ryzyko związane z przetwarzaniem danych osobowych można uznać za znikome i akceptowalne. Ponadto, administrator danych osobowych będzie na bieżąco reagował na wszelkie pojawiające się potencjalne zagrożenia i ryzyka, dostosowując swoje procedury.