RODO

LUXCONTROL POLSKA

Polityka bezpieczeństwa przetwarzania danych osobowych

Luxcontrol Polska
Centrum Pomiarów Bezpieczeństwa i BHP

RODO

LUXCONTROL POLSKA

§ 1. Podstawowe definicje:

1. **dane osobowe**: wszelkie dane pozwalające na identyfikację ich właściciela, dobrowolnie podane w toku współpracy z Luxcontrol Polska. Gromadzone w trakcie współpracy z nami, dane to: imię i nazwisko, data urodzenia, adres e-mail, numer telefonu, adres, numer konta bankowego i dane banku, wynik egzaminu końcowego, adres IP i dane urządzenia, z którego logowano się do systemu;
2. **przetwarzanie danych osobowych**: zespół czynności przeprowadzonych na danych osobowych w sposób zautomatyzowany lub też nie, polegający na: gromadzeniu danych, ich segregacji, utrwaleniu, zabezpieczeniu, udostępnieniu, usunięciu lub zniszczeniu;
3. **ograniczenie przetwarzania danych**: działanie zmierzające do ograniczenia wykonywania jakichkolwiek zbędnych przetwarzań danych;
4. **profilowanie**: jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
5. **pseudonimizacja**: jest sposobem przetwarzania danych osobowych tak, aby nie można było ich przypisać konkretnej osobie, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
6. **zbiór danych**: jest to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
7. **administrato**r: to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych

osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

8. **podmiot przetwarzający**: to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot przetwarzający dane na polecenie i w imieniu administratora;
9. **odbiorca**: jest osobą fizyczną lub prawną, organem publicznym, jednostkę lub inny podmiotem, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, czy też nie;
10. **naruszenie ochrony danych osobowych**: oznacza naruszenie bezpieczeństwa zbiorów danych, które doprowadziło do: przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
11. **przedstawiciel**: jest osobą fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;
12. **rejestr czynności przetwarzania danych**: jest to rejestr wszystkich rodzajów czynności przetwarzania danych, które realizował administrator danych;
13. **rejestr kategorii czynności przetwarzania**: jest to rejestr wszystkich rodzajów czynności przetwarzania danych, które realizował podmiot przetwarzający dane.

§ 2. Zasady dotyczące przetwarzania danych osobowych:

1. dane przetwarzane są zgodnie z zasadami prawa, w celu określonym i zrozumiałym dla osoby, która dane te w sposób dobrowolny udostępniła,
2. zgromadzone przez Luxcontrol Polska dane przestają być przetwarzane niezwłocznie po zrealizowaniu ustawowo określonego okresu przechowywania dokumentacji szkoleniowej,
3. zgodnie z minimalizacją danych, Luxcontrol gromadzi jedynie dane niezbędne do realizacji procesu szkolenia i wydania oraz wysyłki zaświadczenia,
4. Luxcontrol Polska oświadcza, że podanie danych osobowych przez uczestników szkolenia jest dobrowolne, zgoda na przetwarzanie danych może zostać cofnięta w dowolnym momencie współpracy, co może jednak skutkować przerwaniem szkolenia,
5. posiadane przez Luxcontrol Polska dane podlegają ochronie przed niezgodnym z prawem zniszczeniu, utratą, modyfikacją lub nieuprawnionemu przetwarzaniu,

6. osoba, której dane dotyczą ma prawo do wglądu w te dane, wniosku o ich sprostowanie, usunięcie lub pseudonimizację,
7. osoba, której dane są w posiadaniu Luxcontrol Polska ma prawo skargi do organu nadrzędnego na sposób przetwarzania danych osobowych,
8. osoby, których danymi dysponuje Luxcontrol Polska mają prawo do kontaktu z Inspektorem Ochrony Danych, Panem Krzysztofem Trześniewskim dostępnym pod: adresem e-mail: iod@luxcontrol.pl, numerem telefonu: 502-931-844,

§ 3. Środki ochrony danych osobowych w firmie:

1. pracownicy Luxcontrol są zobowiązani do zachowania najwyższych standardów bezpieczeństwa podczas kontaktu z danymi osobowymi,
2. zabrania się przekazywania przez telefon jakichkolwiek danych osobowych,
3. zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych,
4. zabrania się wyrzucania, bez uprzedniego zniszczenia, dokumentów zawierających dane osobowe,
5. należy zapewnić bezpieczne przekazywanie papierowych dokumentów zawierających dane osobowe. Dokumenty kadrowo-płacowe powinny być oddzielone od pozostałych i zabezpieczone przed dostępem osób postronnych w sposób określony w Kodeksie Pracy,
6. w trakcie wykonywania pracy, pracownicy są zobowiązani do utrzymania polityki tak zwanego czystego biurka, tak aby potencjalny klient lub inna osoba odwiedzająca biuro nie miała wglądu w dane osobowe, będące w posiadaniu pracownika,
7. pracownicy są zobowiązani do przestrzegania bezpieczeństwa przetwarzanych danych osobowych poprzez zabezpieczenie ich integralności, dostępności i poufności, w szczególności zabezpieczania dokumentów oraz nośników przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy np. przez zamykanie w szafach, biurkach, pomieszczeniach.

§ 4. Środki ochrony danych osobowych w firmie podczas korzystania z komputerów, internetu i systemów informatycznych:

1. każdy z pracowników jest zobowiązany do posługiwania się własnym loginem do platform internetowych, których używa w trakcie pracy do przetwarzania danych osobowych,
2. zabrania się posługiwania i pracy cudzym loginem,
3. należy ograniczyć do niezbędnego minimum podłączanie i korzystanie z prywatnych pendrive'ów USB, płyt CD/DVD w służbowych komputerach,
4. nie należy otwierać załączników do wiadomości e-mail z niezaufanego źródła,
5. zabrania się otwierania hiperłączy z nieznanego lub niezaufanego źródła przesłanych w wiadomości e-mail lub za pośrednictwem social mediów firmy,
6. zabrania się przesyłania w postaci niezaszyfrowanych załączników e-mail danych osobowych,
7. pracownikom nakazuje się co najmniej raz w miesiącu zmieniać hasło logowania do platform, w których mają oni dostęp do danych osobowych,
8. zabrania się zapisywania haseł do platform w przeglądarkach internetowych,
9. zabrania się przekazywania haseł do logowania innym użytkownikom,
10. w sytuacji kiedy zachodzi podejrzenie, że hasło straciło przymiot poufności lub pracownik podejrzewa taki stan rzeczy (przechwycenie hasła przez osobę nieuprawnioną) bezwzględnie jest on zobowiązany do niezwłocznej zmiany tego hasła oraz poinformowanie Administratora danych o zaistniałym incydencie,
11. zabrania się wyłączania oraz jakichkolwiek ingerencji w działanie systemów antywirusowych i zapór typu firewall,
12. zabrania się wykorzystywania komputerów służbowych do jakichkolwiek działań sprzecznych z prawem,
13. zabrania się instalowania na komputerach służbowych jakichkolwiek programów pochodzących z nieznanych źródeł,
14. pracownikom nakazuje się korzystanie ze skrzynek poczty e-mail służbowych tylko do wykonywania zadań służbowych,
15. skrzynka służbowa nie powinna być otwarta przez cały czas pracy,
16. pracownicy zobowiązani są do okresowego usuwania korespondencji e-mail zawierającej dane osobowe,

17. należy uważać na załączniki w plikach (.zip, .xlsm, .exe) w mailach od nieznanych nadawców, gdyż jest to potencjalny wirus,
18. pracownicy są zobowiązani niezwłocznie poinformować przełożonego o zaistniałych nieprawidłowościach.

§ 5. Obowiązek zgłaszania naruszeń ochrony danych osobowych:

1. Każdy pracownik lub współpracownik zobowiązany jest do niezwłocznego, nie później niż w ciągu 48 godzin, powiadomienia Inspektora Ochrony Danych **Luxcontrol Polska** o przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać co najmniej:
   a) rodzaj naruszenia,
   b) okoliczności naruszenia,
   c) datę i godzinę stwierdzenia naruszenia, informację, jakiego rodzaju danych/kategorii danych osobowych ono dotyczy,
   d) liczby osób, których naruszenie dotyczy,
   e) informację o podjętych działaniach mających na celu minimalizację naruszenia.
3. Za sytuację wymagającą zgłoszenia uznać należy:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą lub utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników,
   d) wykorzystanie wizerunku zamieszczonego przez Administratora w mediach społecznościowych bez wymaganej zgody.
4. Incydenty wymagające powiadomienia:
   a) zdarzenia losowe zewnętrzne (pożar, zalanie wodą, utrata zasilania),
   b) zdarzenia losowe wewnętrzne (awarie komputerów, twardych dysków, utrata /zagubienie danych),
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych /sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów /danych).
5. Najczęstsze przykłady incydentów wymagające reakcji:

a) ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
b) ustawienie monitorów oraz klawiatur pozwalające na wgląd osób postronnych w dane osobowe,
c) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
d) telefoniczne próby wyłudzenia danych osobowych,
e) kradzież, zagubienie komputerów lub nośników zawierających dane osobowe,
f) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
g) niewłaściwe przechowywanie haseł np. hasło przyklejone pod klawiaturą.

Piła, dnia 24 maja 2018 roku

Zatwierdzam wprowadzenie zasad Polityki zasad przetwarzania danych osobowych

KRZYSZTOF TRZEŚNIEWSKI

(pieczęć i podpis Administratora danych osobowych)