Друштво за производство, санација и инжињеринг
КЕДИНГ ДООЕЛ
Бр. 12-59/6
28.02.2022 год.
Скопје

www.keding.com.mk

П О Л И Т И К А З А Н А Р У Ш У В А Њ Е Н А Б Е З Б Е Д Н О С Т А
- ДПСИ Кединг ДООЕЛ СКОПЈЕ -

Февруари, 2022
- 1 Издание -

Управителот на ДПСИ Кединг ДООЕЛ Скопје на ден 28.02.2022 година, за потребата од усвојување на Политика за пријава на нарушување на безбедноста на личните податоци согласно новиот Закон за заштита на личните податоци усвоен на 16.02.2020 година од Собранието на РМ („Службен весник на Република Македонија" бр. 42/20) и член 90 став 2 од Законот, ја донесе следната:

П О Л И Т И К А
за пријава на нарушување на безбедноста на личните податоци

I. ЦЕЛ НА ПОЛИТИКАТА

Друштвото е целосно запознато со своите обврски согласно Законот за заштита на личните податоци за законска обработка на личните податоци и за потребата од осигурување дека личните податоци на субјектите на лични податоци се безбедни. Друштвото сериозно ги сфаќа своите законски обврски и има предвидено соодветни политки и процедури за да се осигура дека податоците не се подложни на загуби или која било друга злоупотреба.

Законот за заштита на личните податоци предвидува и обврска во случај на нарушување на безбедноста на личните податоци да биде известена Агенцијата за заштита на личните податоци, а во одредени случаи и самиот субјект на личните податоци. Оваа Политика го утврдува начинот на кој Друштвото презема активности доколку се случи некое нарушување согласно Законот за заштита на личните податоци.

II. НАРУШУВАЊЕ НА ЛИЧНИТЕ ПОДАТОЦИ

Нарушување на личните податоци претставува нарушување на безбедноста што доведува до случајно или незаконско уништување, губење, промена, неовластено откривање или неовластен пристап до личните податоци, кои се обработени, пренесени или чувани во Друштвото. Нарушувањето во ваква смисла се идентификува како безбедносен инцидент што влијае на трите безбедносни столбови: доверливоста, интегритетот или достапноста на личните податоци.

Нарушувањето на безбедноста на личните податоци во оваа смисла треба да се сфати пошироко, отколку само како губење на податоците. Примери за нарушување на податоци:

- Пристап од неовластено трето лице;
- Активност преземена намерно или од небрежност (или непреземање на активности) од контролорот или обработувачот;
- Испраќање на лични податоци до погрешен примател;
- Украдени или изгубени електронски уреди кои содржат лични податоци;
- Промена на личните податоци без дозвола;
- Губење на достапноста на личните податоци.

III. МЕРКИ ЗА ОТКРИВАЊЕ НА НАРУШУВАЊАТА

За навремено откривање на нарушувањата на безбедноста на личните податоци ги спроведовме следниве мерки:

Ризикот за пристап од неовластени лица до работните единици (компјутерите) на кои се обработуваат личните податоци ќе се надмине преку спроведување на следниве технички мерки:

- на влезот на канцеларииите каде во хартиена форма се чуваат лични податоци е назначено дека ВЛЕЗОТ Е ЗАБРАНЕТ, ОСВЕН ЗА ОВЛАСТЕНИ ЛИЦА

- кон работните единици (компјутерите) на кои се обработуваат личните податоци, пристапот е возможен само преку авторизација со внес на лозинка на овластеното лице, која се состои од најмалку 8 алфанумерички знаци, од кои најмалку еден е голема буква и специјален знак;

Со цел заштита од злоупотреба на лозинките, истата се менува на период од 90 дена праќа автоматска порака до овластеното лице за промена на лозинката и нема можност овластеното лице да не ја промени лозинката, доколку сака да пристапи до работната единица за обработка на личните податоци.

Дополнително, повторно во насока на заштита од злоупотреба на личните податоци, работната единица преминува во sleep mode, по период на неактивност од 15 минути, по што за повторен пристап се бара автентикација на работната единица.

Во случај било која од работните единици да биде компромитирана, ИТ Администраторот има можност да изврши испитување со кое ќе го пронајде изворот или било каква трага од упадот во информацискиот систем на Друштвото, со цел да се открие дали се загрозени и други елементи.

Друштвото има инсталирано заштитен sид и ги има ограничено портите за комуникација само на оние кои се неопходни за програмите да можат нормално да функционираат, а има и антивирусен софтвер кој автоматски се ажурира, со што се обезбедува сигурноста на работните единици и се превенираат упадите.

Друштвото задолжително пропишува и применува технички и организациски мерки во посебен акт во кој се предвидени организациските и техничките мерки преку кои се обезбедува безбедна обработка на личните податоци и врши спроведување и проверка на планираните мерки, а со цел да се обезбеди дека тие се применуваат и тековно се тестираат. Друштвото задолжително спроведува периодични безбедносни проверки предвидени во акциониот план, чија имплементација се следи од страна на раководството на Друштвото и Офицерот за заштита на личните податоци.

IV. ОБВРСКА ЗА ИЗВЕСТУВАЊЕ ЗА НАРУШУВАЊА

За целите на оваа политика, предмет на известување се нарушувања на безбедноста на личните податоци кои Друштвото смета дека претставуваат ризик за правата и слободите на субјектот на личните податоци. Доколку нарушувањето не го носи тој ризик, нарушувањето не е предмет на известување, иако истото ќе биде заведено во Записник за нарушувања и во евиденцијата за нарушувања на безбедноста.

Ризикот по слободите и правата на субјектите на лични податоци, може да вклучи материјална или нематеријална штета, како што е дискриминација, кражба на идентитет, измама, финансиска загуба или нарушување на угледот.

При проценка на веројатноста за ризик по правата и слободите на поединецот, Друштвото најмногу ќе се осврне на:

- Видот на нарушување;
- Видот на личните податоци предмет на нарушување, и што тие податоци претставуваат за субјектот на личните податоци;
- Колку податоци се предмет на нарушување;
- На кого се однесуваат личните податоци, т.е. колку физички лица се вклучени, дали и колку лесно може да се идентификуваат, дали станува збор за податоци за деца, дали станува збор за посебни категории на лични податоци и слично;
- Какви се/какви можат да бидат последиците за субјектите на личните податоци на кои се однесуваат податоците и
- Природата на работата на Друштвото и влијанието на нарушувањето на самото Друштво.

V. ПРЕЗЕМАЊЕ НА АКТИВНОСТИ ПО УТВРДУВАЊЕ НА НАРУШУВАЊЕ

Кога Друштвото ќе дознае за нарушувањето на безбедноста, ќе ги преземе сите активности за отпочнување на истрага за да дознае што се случило и кои активности треба да се преземат за да се ограничат понатамошните последици. Истовремено, ќе се утврди и дали нарушувањето се смета за нарушување за кое треба да се извести Агенцијата за заштита на личните податоци и дали претставува висок ризик за правата и слободите на субјектот на личните податоци.

VI. ВРЕМЕНСКИ РОКОВИ ЗА ИЗВЕСТУВАЊЕ НА АГЕНЦИЈАТА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Во случај да во Друштвото се случи нарушување на безбедноста на личните податоци за кои треба да се извести Агенцијата за заштита на личните податоци („**Агенцијата**“), Друштвото ќе ја извести Агенцијата без непотребно одлагање, а најдоцна во рок од 72 часа од моментот кога дознала за нарушување на безбедноста на

личните податоци. Доколку овој рок за известување од било која причина се надмине, а по правило не смее да се надмине, во таков случај Друштвото во најкус можен рок ќе ја извести Агенцијата за причините.

Ако не е можно да се спроведе целосна истрага за нарушувањето со цел да се дадат целосни детали до Агенцијата во рок од 72 часа, првичното известување ќе се изврши во предвидениот рок, обезбедувајќи што е можно повеќе детали, заедно со причината за нецелосното известување и проценетата временска рамка за целосно известување до надлежниот орган. Првичното известување ќе биде проследено со дополнителна комуникација до Агенцијата за да Друштвото ги достави преостанатите информации кои се добиени по првичното известување.

VI. СОДРЖИНА НА ИЗВЕСТУВАЊЕТО ЗА НАРУШУВАЊЕ ДО АГЕНЦИЈАТА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Известувањето мора да ги содржи следниве податоци:

- опис на природата на нарушувањето на безбедноста на личните податоци, вклучувајќи ги и категориите и приближниот број на засегнати субјекти на личните податоци, како и категориите и приближниот број на засегнати евидентирани лични податоци;
- наведување на името, презимето и контакт податоците на Офицерот за заштита на личните податоци или на друго лице за контакт, од кое може да се добијат повеќе информации;
- опис на можните последици од нарушувањето на безбедноста и
- опис на преземените или предложените мерки од страна на Друштвото во улога на Контролор за справување со нарушувањето на безбедноста на личните податоци, вклучувајќи и соодветни мерки за намалување на можните негативни ефекти.

VII. ВРЕМЕНСКИ РОКОВИ ЗА ИЗВЕСТУВАЊЕ ДО СУБЈЕКТОТ НА ЛИЧНИТЕ ПОДАТОЦИ

Кога нарушувањето се смета дека е предмет на известување и кога се смета дека претставува висок ризик за правата и слободите на поедниците, Друштвото покрај Агенцијата, веднаш ќе ги извести и самите засеганти лица односно субјекти на личните податоци, ако тоа е возможно.

Висок ризик во смисла на оваа политика, на пример може да биде, непосредна закана за кражба на идентитет, или откривање на посебни категории на лични податоци на интернет.

VIII. СОДРЖИНА НА ИЗВЕСТУВАЊЕТО ЗА НАРУШУВАЊЕ ДО СУБЈЕКТОТ НА ЛИЧНИТЕ ПОДАТОЦИ

Известувањето за нарушување на безбедноста на личните податоци, кое Друштвото го праќа до субјектот на личните податоци, мора да ги содржи следниве податоци:

- опис на природата на нарушувањето;
- име, презиме и контакт од овластеното лице за заштита на личните податоци, со информација каде може да се добијат повеќе информации;
- опис на веројатните последици од нарушувањето на безбедноста на личните податоци и
- опис на преземените мерки или предложените мерки за справување со нарушувањето на безбедноста и каде што е соодветно, мерките преземени за ублажување на евентуалните негативни ефекти.

Известувањето до субјектот на личните податоци од оваа политика не е задолжително, доколку е исполнет еден од следните услови:

- Друштвото применило соодветни технички и организациски мерки за заштита и тие мерки биле применети во однос на личните податоци засегнати од нарушувањето на безбедноста на личните податоци, особено мерки коишто ги прават личните податоци неразбирливи за секое лице кое нема овластување за пристап до нив, како што е криптирањето;
- Друштвото применило дополнителни мерки кои гарантираат дека веќе не постои веројатност за појавување на висок ризик за правата и слободите на субјектите на личните податоци од оваа политика;

- Ако за известувањето е потребен несразмерен напор. Во таков случај, се врши јавно известување или се применува друга слична мерка со која субјектите на личните податоци ќе бидат подеднакво информирани на ефикасен начин.

IX. ДОКУМЕНТИРАЊЕ НА НАРУШУВАЊАТА

Друштвото ги документира, односно ги евидентира сите нарушувања на безбедноста, без оглед дали тие се предмет на известување или не, како дел од обврските за отчетност според Законот за заштита на личните податоци. Во евиденцијата ги бележи фактите во врска со нарушувањето, ефектите и преземените мерки. Оваа евиденција е достапна за Агенцијата при супервизија над работата на Друштвото.

Управител

Габриел Кедиоски

Друштво за производство, санација и инжинеринг КЕДИНГ ДООЕЛ 1 СКОПЈЕ