



Друштво за производство, санација и инжињеринг

КЕДИНГ ДООЕЛ

Бр. 12 - 59/15

18.02. 2022 год.
Скопје

www.keding.com.mk

ПОЛИТИКА ЗА ПРЕНОС НА ЛИЧНИТЕ ПОДАТОЦИ

- 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 пренос 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:

ПОЛИТИКА ЗА ПРЕНОС НА ЛИЧНИТЕ ПОДАТОЦИ

Во ДПСИ Кединг ДООЕЛ Скопје поголемиот дел од личните податоци се обработуваат во електронска форма, а истите се чуваат како во електронска, така и во хартиена форма. Оваа Политика ги регулира процедурите за заштита на личните податоци и утврдува како истите треба да се пренесуваат во и надвор од Друштвото, на безбеден и заштитен начин.

Овластено лице за заштита на личните податоци е Офицерот за заштита на личните податоци, Јасмина Арбелска, e-mail: jasmina.a@keding.com.mk.

I. ЗАКОН

Чувањето на личните податоци е уредено со Законот за заштита на личните податоци. Клучно во ЗЗЛП е тоа дека личните податоци можат да бидат пренесени во земјите на ЕУ и ЕЕЗ, но не и во трети земји, освен во случај таа земја да обезбедува соодветни заштитни мерки.

II. ЧУВСТВИТЕЛНИ ПОДАТОЦИ

Чувствителни податоци, за целите на оваа политика, вклучуваат податоци кои содржат:

- Лични податоци за поединецот (вклучително и оние податоци кои се класифицирани како посебни категории на лични податоци, а кои се однесуваат на здравјето, расата, етничката припадност, итн...);
- Доверливи податоци за Друштвото;
- Доверливи податоци за стоки, производи и услуги;
- Доверливи податоци за клиентите и добавувачите на Друштвото.

Доколку вработениот има сомневање дали податоците се чувствителни или не, мора да се обрати до непосредниот Директор на РЕ / Сектор / Служба.

III. ПРЕНОС НА ПОДАТОЦИ

Вработените мора да побараат согласност од Управителот, за да се одобри трансфер на чувствителни податоци.

Податоците (без разлика дали се чувствителни) треба да се пренесуваат само тогаш кога е строго неопходно за ефективното работење на Друштвото. Следствено, пред да се побара одобрение за пренос, треба да се утврди дали е неопходен трансферот на податоците.

Доколку се работи за меѓународен пренос на лични податоци, вработениот задолжен за истото мора првично да утврди во која земја/и ќе се врши преносот на личните податоци. Потоа, мора да утврди дали е строго неопходно да се пренесат податоците во таа/тие земја/и, и да побара одобрение од Директорот на Секторот за правни, кадрови и општи работи, за преносот. По добивање на одобрението, доколку се работи за пренос на податоци во земја/и на ЕУ или ЕЕЗ, тогаш мора да се извести офицерот за заштита на личните податоци, кој е должен преносот да го пријави во АЗЛП. Доколку се работи за пренос на податоци во трета земја, вработениот повторно го известува Офицерот за потребата од преносот и сите информации кои му се потребни на Офицерот за да подготви и достави барање за одобрување на преносот до АЗЛП. Вработениот нема да го изврши преносот пред добивање на одобрение од страна на Офицерот дека сите законски обврски се исполнети.

IV. ПРЕНОС НА ПОДАТОЦИ ПРЕКУ ПОШТА / КУРИР

Пренос на податоци кои мора да се достават преку медиуми, како што се мемориски картички, УСБ стик, ЦД или хард-диск, мора да се достават само преку безбедна и лиценцирана пошта. Истите треба да бидат доставени и обвиткани на начин што ќе бидат заштитени од кршење или уништување за време на нивниот пренос и ќе може да се утврди дали истите се отворени пред да стигнат до нивната финална дестинација.

Примателот мора да биде јасно наведен во писмото.

Примателот треба да биде известен однапред за да ги очекува податоците. Примателот мора да потврди безбеден прием на пратката веднаш штом ќе пристигнат податоците. Вработениот одговорен да ги достави податоците е одговорен за потврда дека податоците пристигнале безбедно и за споделување на лозинките со примателот.

V. ИЗГУБЕНИ ИЛИ ИСЧЕЗНАТИ ПОДАТОЦИ

Доколку вработен утврди дека некои податоци се изгубени или недостасуваат, од него се бара веднаш да го извести Управителот или Офицерот за заштита на лични податоци.

Политиката за известување на нарушување на безбедноста ќе биде активирана и следена од страна на Друштвото. Друштвото е должно веднаш, без одолговлекување, да отпочне истрага за да утврди како се случила кражба/губење на податоци и да се утврди дали има нарушување на безбедноста во Друштвото. Доколку позитивно се одговори на тоа прашање, врз основа на таа Политика ќе се утврди дали ги исполнува предвидените услови за да се известат Агенцијата за заштита на личните податоци и субјектот на личните податоци.

Управителот мора да ја разгледа опцијата да повика полиција, доколку се утврди дека неовластени лица имале пристап до чувствителните податоци утврдени со оваа Политика.

VI. НЕВНИМАТЕЛЕН ПРЕНОС НА ЛИЧНИ ПОДАТОЦИ

Постапките на вработените кои не ги почитуваат задолжувањата, односно обврските утврдени во оваа Политика, ќе се сметаат за грубо кршење на работните обврски, што може да резултира со отказ од работното место. Нарушувањето на безбедноста на личните податоци може да резултира со исклучително драстични санкции за Друштвото.

Вработените не смеат да бидат невнимателни при пренесување на чувствителни податоци. Како примери за невнимателност се следниве: недобивање одобрение од Управителот; необезбедување шифрирање, компресирање и заштита на личните податоци од ИТ Администраторот на Друштвото; користење на небезбедени поштенски услуги кои не се следат или не се осигурани; или неизвестување на Офицерот за заштита на личните податоци за трансферот на податоци надвор од нашата земја.

Управител

Габриел Кедиоски

