Технички и организациски мерки на ДПТУ Милд ДООЕЛ Струмица

Со овој документ се пропишуваат техничките и организациски мерки за обезбедување тајност и заштита на личните податоци што се применуваат Милд, а кои произлегуваат од законската обврска на ДПТУ МИЛД ДООЕЛ Струмица (во понатамошен текст Милд) за следење и примена на Законот за заштита на личните податоци, како и Правилникот за технички и организициски мерки за обезбедување тајност и заштита на обработката на личните податоци.

Обработка на лични податоци

Системот за технички и организациски мерки за обезбедување на тајност и заштита на обработката на личните податоци е усогласен на видот и обемот на личните податоци што се обработуваат во Милд.

Милд обработува збирки на лични податоци за вработени и и збирки на лични податоци за корисници на производите на Милд. Офицерот за заштита на лични податоци е одговорен за ажурирањето на Листата на збирки на лични податоци.

Категориите на лични податоци содржани во збирките на лични податоци се обработуваат врз основа на закон или врз основа на согласност на субјектот на лични податоци.

Подготовка и ажурирање на документација за технички и организациски мерки

Милд подготвува, донесува и имплементира документација за технички и организациски мерки со цел да се обезбеди функционален систем на технички и организациски мерки за тајност и заштита на обработката на личните податоци.

Документацијата ја сочинуваат:

- План за создавање систем на технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци
- Правила за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци
- Правила за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите
- Правила за определување на обврските и одговорностите на администраторите на информациските системи и на овластените лица при пристапувањето до документите и информатичко комуникациската опрема.
- Правила за пријавување, реакција и санирање на инциденти

Одржување на информацискиот систем

Физичките или правните лица кои вршат одржување на информациските системи на Милд, при што обработуваат лични податоци на Милд, треба да постапуваат согласно прописите за заштита на личните податоци и донесената документација за технички и организациски мерки.

Технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци

Правилата дефинирани подолу произлегуваат од законската обврска утврдена во Законот за заштита на личните податоци, како и Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци на Агенцијата за заштита на личните податоци, според кои Милд треба да применува технички и организациски мерки кои обезбедуваат тајност и заштита на обработката на личните податоци, соодветно на природата на податоците кои се обработуваат и ризикот при нивната обработка и истите се класифицираат во три нивоа:

- Основно
- Средно
- Високо

Насоки за примена на нивоата:

- За сите документи задолжително се применуваат технички и организациски мерки кои се класифицирани на основно ниво
- За документи кои содржат: посебни категории на лични податоци , задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво
- За документите кои содржат единствен матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво
- За документите кои се пренесуваат преку електронско комуникациска мрежа, а содржат посебни категории на лични податоци и единствен матичен број на граѓанинот, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво

Основно ниво на технички и организациски мерки

Технички мерки

Милд обезбедува соодветни технички мерки за тајност и заштита на обработката на личните податоци кои се однесуваат на следните барања:

- Единствено корисничко име
- Лозинка креирана од секое овластено лице кое пристапува до информацискиот систем, составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци
- Корисничко име и лозинка која овозможува пристап на овластеното лице до информацискиот систем во целина, до поединечни апликации и/или поединечни збирки на лични податоци потребни за извршување на неговата работа
- Автоматизирано одјавување од информацискиот систем после изминување на определен период на неактивност (не подолго од 15 минути)

- Автоматизирано отфрлање од информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка)

- Инсталирана хардверска/софтверска заштитна мрежна бариера (“firewall”) или рутер помеѓу информациските системи и интернет или било која друга форма на надворешна мрежа

- Ефективна и сигурна анти-вирусна, анти–спајвер и анти-спам заштита на информациските системи, која постојано ќе се ажурира заради превентива од непознати и непланирани закани од нови вируси, спајвери и спамови.

- Приклучување на информациските системи (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување

Организациски мерки

Милд обезбедува соодветни организациски мерки за тајност и заштита на обработката на личните кои се однесуваат на следните барања:

- Ограничен пристап или идентификација за пристап до личните податоци

- Организациски правила за пристап на овластените лица до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и други извори

- Уништување на документи по истекот на рокот за нивно чување

- Мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци

- Почитување на техничките упатства при инсталирање и користење на информатичко комуникациската опрема на која се обработуваат личните податоци

Физичка сигурност на информацискиот систем

Дел од серверите на кои се инсталирани софтверските програми за обработка на личните податоци се физички лоцирани и хостирани во Милд, како и администрирани од страна на Милд , а дел се хостирани од надворешен партнер на Милд. Партнерите на Милд се обврзани да ги почитуваат минимум барањата за физичка сигурност на информацискиот систем.

Физички пристап до просторијата во која се сместени серверите имаат само овластени лица од Милд. Доколку е потребен пристап на друго лице до просторијата и личните податоци зачувани на серверите, тогаш тоа лице е придружувано и надгледувано од овластено лице.

Просторијата во која се сместени серверите се заштитува од ризиците во опкружувањето преку примена на мерки и контроли со кои се намалува ризикот од потенцијални закани вклучувајќи кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

Информирање за заштитата на личните податоци

Лицата кои се вработуваат во Милд, по потпишување на Договорот за работа, своерачно потпишуваат и Изјава за почитување на правилата за користење на ИТ ресурси и Изјава за почитување на деловна тајна, за сите податоци до кои ќе дојдат во допир при извршување на работните задачи. Со потпишувањето на изјавата, вработените во Милд се обврзуваат да ги

почитуваат сите усвоени регулативи во Милд кои директно или индиректно се однесуваат на обработка на лични податоци. Милд се обврзува континуирано да врши информирање на вработените и ангажираните лица за непосредните обврски и одговорности за заштита на личните податоци, преку оддржување на обуки за заштита на личните податоци.

За лицата вработени кај друг работодавач - давател на услуги на Милд, сите надворешни консултанти, обучувачи и сите лица што работат Милд, обврските и одговорностите за заштита на личните податоци се регулираат со посебен договор или во договорот со кој се уредува деловниот однос меѓу Милд и давателот на услуги на Милд.

Идентификација и проверка

Милд задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и информациските системи, како и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

Кога проверката се врши врз основа на корисничко име и лозинка, Милд секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите.

Средно ниво на технички и организациски мерки

Контрола на информацискиот систем и информатичката инфраструктура

Милд спроведува безбедносни проверки и ревизии, како и проверки на степенот на заштита на личните податоци, на редовна основа со вклученост на офицерот за заштита на лични податоци и други лица кои му помагаат на офицерот при извршување на овие контроли.

Надворешна контрола

Информациските системи и информатичката инфраструктура на Милд подлежат на надворешна контрола, преку обработка на документи од страна на независно трето правно лице, која се спроведува секои три години, а со цел да се провери дали постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на лични податоци.

Идентификација и проверка

Милд има воспоставено механизми кои овозможуваат јасна идентификација на секое овластено лице кое пристапило до информацискиот систем и можност за проверка на неговата/нејзината авторизација.

Евидентирање на авторизираниот пристап

Милд води евиденција за секој авторизиран пристап која треба да ги содржи особено следните податоци:

- име и презиме на овластеното лице,
- работна станица од каде се пристапува до информацискиот систем,
- датум и време на пристапување,
- лични податоци кон кои е пристапено,
- видот на пристапот со операциите кои се преземени при обработка на податоците,
- запис за авторизација за секое пристапување,
- запис за секој неавторизиран пристап и

- запис за автоматизирано отфрлање од информацискиот систем.

Во евиденцијата се внесуваат и податоци за идентификување на информацискиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво на авторизација.

Тестирање на информацискиот систем

Одговорната организациска единица во Милд, задолжително врши тестирање на информациските системи пред нивното имплементирање или по извршените промени со цел да се провери дали системот обезбедува тајност и заштита на обработката на личните податоци согласно со документацијата за технички и организациски мерки и прописите за заштита на личните податоци.

Високо ниво на технички и организациски мерки

Пренесување на личните податоци преку електронско комуникациска мрежа

Личните податоци можат да се пренесуваат преку електронско комуникациска мрежа само ако се криптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи при преносот.

Правила при рачна обработка на личните податоци

Основно, средно и високо ниво на технички и организациски мерки

Рачната обработка на личните податоци кои се класифицирани со основно, средно или високо ниво во однос на:

- Пристапот до документи
- Правилото чисто биро
- Чување на документите
- Копирање или умножување на документите и
- Пренесување на докумети

Уништување, бришење или чистење на документите и медиумите

Уништувањето или бришењето на документите и медиумите на кои има лични податоци кои се категоризирани во основно ниво на заштита се прави на тој начин што истите не би можеле да се репродуцираат или вратат, односно на начин кој што ќе оневозможи понатамошно обновување на личните податоци (на пример: со користење на шредер).

Уништувањето или бришењето на документите и медиумите на кои има лични податоци, кои се категоризирани во средно и високо ниво на заштита треба да се прави на тој начин што истите не би можела да се репродуцираат или вратат, односно на начин што ќе оневозможи понатамошно обновување на снимените лични податоци (на пример со користење на шредер).

Електронското бришење на личните податоци кое се врши при редовното оперативно работење се евидентира во логови кои содржат информација за времето на настанот и лицето кое го направило тоа.

Бришењето и уништувањето мора да се направи комисиски, во присуство на 3 члена, при што задолжително се изготвува Записник кој треба да ги содржи следните информации:

- Времето на бришењето/уништувањето на податоците
- Местото на бришење/уништување на податоците
- Начинот на бришење/уништување на податоците (со шредер, електронски, преку надворешна фирма и сл.)
- Типот и категоријата на податоците
- Причината заради која се бришат/уништуваат податоците
- Лицата кои вршат бришење/уништување на податоците

Записникот за уништување и бришење на документите и медиумите се чува и во електронска форма во временски период од 5 години.

Технички мерки за обезбедување на веб-страницата

Милд применува технички мерки со кои се гарантира доверливостана информациите што ги испраќа или ги собира преку веб-страницата, и тоа особенопреку следните мерки:

- имплементација на криптографски протокол (TLS) на веб страницата

- обезбедува дека само овластени лица кои имаат администраторски привилегии ќе можат да имаат пристап до веб страницата и алатките потребни за нејзина администрација

- Обезбедување на согласност за користење на колачиња, со соодветно известување за корисникот

Милд во ниту еден случај:

- Не пренесува лични податоци преку URL без примена на протокол за криптирање

(на пример идентификатори или лозинки);

- Не користи услуги кои знае или треба да знае дека се небезбедни;

- Не ги поставува базите на податоци на сервери кои се директно достапни преку

интернет; и

- Не споделува корисничките сметки (user accounts) помеѓу две или повеќе овластени лица.