Врз основа на член 105 од Законот за основното образование („Службен весник на Република Северна Македонија" бр. 161/19 и 229/2020), министерот за образование и наука донесе

ПРАВИЛНИК
ЗА НАЧИНОТ НА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ, ЛИЦАТА КОИ СЕ ОВЛАСТЕНИ ДА ГИ КОРИСТАТ ПОДАТОЦИТЕ СОДРЖАНИ ВО ПОЕДИНЕЧНИТЕ ЗБИРКИ НА ЛИЧНИ ПОДАТОЦИ, КРИТЕРИУМИТЕ СПОРЕД КОИ СЕ УТВРДУВА НИВОТО НА ПРИСТАП НА ЛИЦАТА КОИ СЕ ОВЛАСТЕНИ ДА ГИ ОБРАБОТУВААТ ЛИЧНИТЕ ПОДАТОЦИ, ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ, НАЧИНОТ НА УНИШТУВАЊЕ ПО ИСТЕКУВАЊЕТО НА РОКОТ НА ЧУВАЊЕ НА ЛИЧНИТЕ ПОДАТОЦИ И ДРУГИ МЕРКИ

Член 1

Со овој правилник се пропишува начинот на обработка на личните податоци, лицата кои се овластени да ги користат податоците содржани во поединечните збирки на лични податоци, критериумите според кои се утврдува нивото на пристап на лицата кои се овластени да ги обработуваат личните податоци, техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, начинот на уништување по истекувањето на рокот на чување на личните податоци и други мерки.

Начин на обработка на личните податоци

Член 2

Збирката на податоци за учениците запишани во основното училиште, збирката на податоци за деца што се на училишна возраст а не се запишани во училиште и збирката на податоци за родители, односно старатели на ученици запишани во основното училиште овластеното лице ги добива од раководителот на паралелката во која ученикот е запишан.

Збирката на податоци за вработените во основното училиште овластеното лице ги добива од одговорното лице за кадровски работи во основното училиште.

Овластени лица за обработка на податоците содржани во поединечните збирки на лични податоци

Член 3

Училиштето (Во понатамошниот текст: контролорот) ги утврдува овластените лица кои треба да имаат пристап до информацискиот систем при што обезбедува јасна поделба на должностите и одговорностите според правилото „потребно е да знае".

Овластените лица задолжително имаат авторизиран пристап само до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работни задачи.

Контролорот обезбедува повлекување на правата на пристап веднаш по престанокот на овластувањата за пристап.

Контролорот врши проверка и ажурирање на привилегиите за пристап до информацискиот систем на овластените лица. Проверката се врши за периоди кои се определуваат врз основа на анализата на ризикот, а најмалку квартално.

За планирање и за применување на технички и организациски мерки, како и за контрола на обезбедувањето тајност и заштита на обработката на личните податоци, контролорот именува администратор на информацискиот систем во училиштето (Во понатамошниот текст: Администратор).

Администраторот од став (1) на овој член, врши планирање и применување на технички и организациски мерки, како и контрола на обезбедувањето тајност и заштита на обработката на

личните податоци во училиштето, а во согласност со член 36 од Законот за заштита на личните податоци

Администраторот задолжително има авторизиран пристап само до личните податоци и информатичко комуникациската опрема која е неопходна за извршување на неговите работни задачи.

Контролорот воспоставува механизми за да се оневозможи пристап на овластените лица до личните податоци и информатичко комуникациската опрема со права различни од тие за кои се авторизирани.

Администраторот, ги доделува, менува или одзема привилегиите на авторизираниот пристап до личните податоци и информатичко комуникациската опрема само во согласност со критериумите кои се утврдени од страна на Контролорот.

Администраторот има познавање на информатички вештини потребни за обработката на личните податоци за учениците запишани во основното училиште, за деца што се на училишна возраст, а не се запишани во училиште, за родителите, односно старателите на учениците запишани во основно училиште и за вработените во основното училиште, и за информатичко комуникациската опрема на кои се обработуваат лични податоци.

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

Член 4

Администраторот, или овластено лице од контролорот се регистрира со единствено корисничко име, електронска адреса и лозинка.

Од страна на системот се врши одобрување за пристап на администраторот, или овластеното лице на податоците содржани во поединечните збирки на лични податоци.

Лозинката е комбинација од најмалку 12 алфанумерички карактери (букви /мали и големи/), симболи, броеви и специјални интерпукциски знаци).

Лозинката се менува на секои 30 дена.

Единственото корисничко име и лозинката овозможуваат пристап на лицата од став 1 на овој член до поединечни апликации и/или поединечни збирки на лични податоци до кои има пристап.

По изминување на определен период на неактивност кој е подолг од 15 минути, се врши автоматизирано одјавување.

По три неуспешни обиди за најавување заради внесување на погрешно корисничко име или лозинка се врши автоматизирано отфрлање од системот по што системот автоматизирано ги известува лицата од став 1 на овој член да креираат нова лозинка за истиот кориснички профил за што системот му испраќа на електронската адреса валидациски линк каде што ја креира новата лозин.

Со цел да обезбеди идентификување на секој неовластен (измамнички) пристап или злоупотреба на лични податоци, како и да се утврди потеклото на овие инциденти, контролорот или лице овластено од него воспоставува и води евиденција за секој пристап до информацискиот систем - logs (на пример: од оперативните системи, од заштитниот sид (firewall), серверот дизајниран специјално за употреба како сервер за датотеки (file server), базите на податоци, системот (софтверот) за управување со документи (DMS System), софтверот за управување со врски со клиенти (CRM Software) и сл;

Евиденцијата од ставот (8) на овој член треба да ги содржи особено следните податоци: име и презиме на овластеното лице, работната 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 од ставот (8) на овој член 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.

За заштита на поединечните збирки на лични податоци се инсталира:
- хардверска/софтверска заштитна мрежна бариера ("firewall") помеѓу информацискиот систем и интернет или било која друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивање на базата на податоци.

За заштита на базата на податоци се врши приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

Серверите на кои се инсталирани софтверските програми за базата на податоци се физички сместени во работните простории на Министерството или надвор од работните простории на Министерството.

Физички пристап до просторијата во која се сместени серверите за базата на податоци имаат само лица посебно овластени од страна на министерот.

Ако е потребен пристап на друго лице до просторијата во која се сместени серверите и личните податоци зачувани на нив, тогаш тоа лице е придружувано и надгледувано од овластеното лице од ставот 2 на овој член, за што се води посебен дневник за пристап на други лица во кој се запишува почетокот и крајот на пристапот, име и презиме на лицето, бројот на личната карта, од кое овластено лице е придружувано и која била целта на неговиот престој во просторијата.

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.

Серверите на кои се инсталирани софтверските програми за базата на податоци се хостирани и администрирани од страна на овластени лица од страна на министерот.

Начин на уништување по истекувањето на рокот на чување на личните податоци и други мерки

Член 5

По истекот на роковите за чување на личните податоци за учениците запишани во основното училиште, личните податоци за родителите, односно старателите на учениците запишани во основно училиште и личните податоци за вработените во основното училиште, администраторот ги брише од базата на податоци.

Член 6

Овој Правилник влегува во сила со денот на неговото донесување.

Бр. 18-8954/1

14.6.2021 година

Скопје

Министер,

Мила Царовска, с.р