Врз основа на член 184 точка б) од Законот за хартии од вредност (Службен весник на Република Северна Македонија бр.95/2005; 25/2007; 7/2008; 57/2010; 135/2011; 13/2013; 188/2013; 43/2014; 15/2015; 154/2015; 192/2015; 23/2016 и 83/2018) и член 23 од Законот за заштита на личните податоци (Службен весник на Република Северна Македонија бр.7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015, 99/2016 и 64/2018), а во врска со член 10 став (2) алинеа 3) од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци (Службен весник на Република Северна Македонија бр.38/2009 и 158/2010), Комисијата за хартии од вредност на Република Северна Македонија на седницата одржана на 10.06.2019 година донесе

ОДЛУКА

за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци

Член 1

Со оваа Одлука се пропишуваат техничките и организациските мерки што Комисијата за хартии од вредност на Република Северна Македонија (во понатамошниот текст: Комисија) во својство на контролор ги применува за да обезбеди тајност и заштита на обработката на личните податоци.

Член 2

Комисијата 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 тоа:

- основно ниво,
- средно ниво и
- високо ниво.

Член 3

Комисијата ја евидентира и ја чува целокупната документација за софтверските програми за обработка на личните податоци и за сите нејзини промени.

Обработка на личните податоци

Член 4

Оваа одлука се применува за:

- целосно и делумно автоматизирана обработка на личните податоци и
- друга рачна обработка на личните податоци, што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Технички мерки

Член 5

Комисијата треба да обезбеди примена на соодветни технички мерки за обезбедување на тајност и заштита на обработката на личните податоци, и тоа:

- единствено корисничко име;

- лозинка креирана за секое овластено лице која е комбинација од најмалку осум алфанумерички занаци и специјални знаци;

- корисничко име и лозинка која овозможува пристап на овластеното лице до информацискиот систем во целина, пристап до поединечни апликации и/или поединечни збирки на личните податоци потребни при извршување на работните задачи;

- автоматизирано одјавување од информацискиот систем по изминување на определен период на неактивност (не подолго од 15 минути), по што за повторно активирање на системот потребно е одново да се внесе корисничкото име и лозинката;

- автоматизирано отфрлање од системот по три неуспешни обиди за пријавување и автоматизирано известување на корисникот дека треба да побара упатство од администраторот на системот;

- инсталирана харверска/софтверска заштитна мрежна бариера („фајервол“) или рутер помеѓу информацискиот систем и интернет мрежата или друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или неовластено пријавување на системот;

- инсталирање на ефективна анти-вирусна и анти-спајвер заштита на информацискиот систем која постојано ќе се ажурира и

- приклучување на информацискиот систем на енергетска мрежа преку уред за непрекинато напојување.

Организациски мерки

Член 6

(1) Комисијата треба да обезбеди соодветни организациски мерки за тајност и заштита на обработката на личните податоци, и тоа:

- ограничен пристап или идентификација за пристап до личните податоци;
- уништување на документи по истекот на рокот за нивно чување согласно прописите за архивска граѓа;
- воспоставување на мерки за физичка сигурност на работните простории и на информатичко-комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци и
- почитување на техничките упатства при инсталирање и користење на информатичко-комуникациската опрема на која се обработуваат личните податоци.

(2) Вработеното лице кое ги врши работите за човечки ресурси во Комисијата го известува администраторот на информацискиот систем за

вработувањето или ангажирањето на секое овластено лице со право на пристап до информацискиот систем, за да му биде доделено корисничко име и лозинка, како и за престанок на вработувањето или ангажирањето за да му бидат избришани корисничкото име и лозинката, односно заклучени за натамошен пристап. Известувањето се врши писмено.

Физичка сигурност на информацискиот систем

Член 7

(1) Серверите, на кои се инсталирани софтверските програми за обработка на личните податоци, се физички лоцирани, хостирани и администрирани од страна на Комисијата.

(2) Физички пристап до просторијата во која се сместени серверите има само администраторот на информацискиот систем.

(3) Доколку е потребен пристап на друго лице до просторијата и личните податоци зачувани на серверите, тогаш тоа лице ќе биде придружувано и надгледувано од лицето од ставот (2) на овој член.

(4) 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.

(5) По исклучок од ставот (1) на овој член, серверите на кои се инсталирани софтверски програми за обработка на личните податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на Комисијата.

(6) Во случајот од ставот (5) на овој член, меѓусебните права и обврски на Комисијата и правното, односно физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите, треба да бидат уредени со договор во писмена форма, кој задолжително ќе содржи технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци.

Офицер за заштита на лични податоци

Член 8

Комисијата овластува офицер за заштита на лични податоци кој ќе биде одговорен за координација и контрола на постапките и упатствата утврдени со техничките и организациските мерки за обезбедување на тајноста и заштитата на обработката на личните податоци.

Информирање за заштитата на личните податоци

Член 9

(1) Лицата кои се вработуваат или се ангажираат во Комисијата, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.

(2) За лицата кои се ангажираат за извршување на работа во Комисијата во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

(3) Комисијата пред непосредното започнување со работа на овластените лица, дополнително ги информира за непосредните обврски и одговорности за заштита на личните податоци.

(4) Лицата кои се вработуваат или се ангажираат во Комисијата, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци која е дадена во прилог на оваа одлука.

(5) Изјавата од ставот (4) на овој член особено содржи: дека лицата ќе ги почитуваат начелата за заштита на личните податоци пред нивниот пристап до личните податоци; ќе вршат обработка на личните податоци согласно упатствата добиени од Комисијата, освен ако со закон поинаку не е уредено и ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита.

(6) Изјавата од ставот (4) на овој член задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат во Комисијата.

(7) Комисијата задолжително врши континуирано информирање на овластените лица за непосредните обврски и одговорности за заштита на личните податоци.

Обврски и одговорности на администраторот на информацискиот систем

Член 10

(1) Обврските и одговорностите на администраторот на информацискиот систем, Комисијата ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.

(2) Офицерот за заштита на личните податоци во Комисијата задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола кој го доставува до Претседателот на Комисијата.

(3) Во извештајот од ставот (2) на овој член треба да се содржани констатираните неправилности доколку такви се констатирани, како и предложените мерки за отстранување на тие неправилности.

Обврски и одговорности на овластените лица

Член 11

(1) Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до информацискиот систем, Комисијата ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.

(2) Комисијата задолжително ги информира овластените лица од ставот (1) на овој член со документацијата за технички и организациски мерки кои се однесуваат на извршувањето на нивните обврски и одговорности.

Идентификација и проверка

Член 12

(1) Комисијата задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и информацискиот систем, како и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

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

(3) Лозинките треба автоматски да се менуваат по изминат временски период што не може да биде подолг од три месеци.

Евиденција на овластените лица кои имаат авторизиран пристап до документите и информацискиот систем

Член 13

Комисијата води евиденција на корисниците кои имаат авторизиран пристап до документите и информатичкиот систем, која содржи:

- Име и презиме на вработениот;
- Работна станица и корисничко име за сите вработени кога пристапуваат до системот, заедно со нивото на авторизиран пристап, датумот и времето на пристапување и личните податоци кон кои е пристапено;
- Видот на пристапот со операциите кои се преземени при обработка на податоците;
- Запис од авторизација за секое пристапување;
- Запис за секој неавторизиран пристап;
- Запис од автоматизирано отфрлање од информацискиот систем.
- Идентификување на систем од кој се врши надворешен обид за пристап во оперативните функции или лични податоци без потребно ниво на авторизација.

Контрола на пристап

Член 14

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

(2) Комисијата 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.

(3) Администраторот на информацискиот систем кој е овластен согласно Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица може да доделува, менува или да го одзема авторизираниот пристап до личните податоци и информатичко-комуникациската опрема само врз основа на налог од страна на Престедателот и во согласност со критериумите кои се утврдени од страна на Комисијата.

Член 15

Одредбите од оваа одлука се применуваат при автоматизирана и при рачна обработка на личните податоци што се дел од постојната збирка на лични податоци во Комисијата.

Контрола на информацискиот систем и информатичката инфраструктура

Член 16

(1) Информацискиот систем и информатичката инфраструктура на Комисијата подлежи на внатрешна и надворешна контрола 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 личните податоци.

(2) Комисијата врши надворешна контрола на информацискиот систем и информатичката инфраструктура на секои три години, а внатрешна контрола секоја година.

(3) Надворешната контрола од став (1) на овој член се врши преку обработка на документи од страна на независно трето правно лице.

(4) Во извештајот од извршената контрола од ставот (1) на овој член задолжително треба да има мислење за тоа во колкава мера постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци, да се наведени констатираните недостатоци, како и предложените неопходни корективни или дополнителни мерки за нивно отстранување.

(5) Во извештајот од ставот (4) на овој член треба да се содржани и податоците и фактите врз основа на кои е изготвено мислењето и се предложени мерките за отстранување на констатираните недостатоци.

(6) Извештајот од ставот (4) на овој член се анализира од страна на офицерот за заштита на личните податоци, кој доставува предлози на контролорот за преземање на потребните корективни или дополнителни мерки, за отстранување на констатираните недостатоци.

Управување со медиуми

Член 17

(1) Пренесувањето на медиумите надвор од работните простории се врши само со претходно писмено овластување од страна на Престедателот на Комисијата.

(2) За пренесените медиуми надвор од работните простории на Комисијата, се преземаат неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.

Уништување, бришење или чистење на медиумот

Член 18

(1) По пренесувањето на личните податоци од медиумот или по истекот на определениот рок за чување, медиумот треба да се уништи, избрише или да се исчисти од личните податоци снимени на него.

(2) Уништувањето на медиумот се врши со механичко разделување на неговите составни делови, при што истиот повторно да не може да биде употреблив.

(3) Бришењето или чистењето на медиумот треба да се изврши на начин што ќе оневозможи понатамошно обновување на снимените лични податоци.

(4) За случаите од ставовите (2) и (3) на овој член комисиски се составува записник, кој ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци снимени на истиот.

Идентификација и проверка

Член 19

Комисијата треба да воспостави механизми кои ќе овозможуваат јасна идентификација на секое овластено лице кое пристапило до информацискиот систем и можност за проверка на авторизацијата за секое овластено лице.

Контрола на физички пристап

Член 20

Во документацијата за технички и организациски мерки, Комисијата определуваа критериуми за овластените лица кои можат да имаат пристап до просториите каде е сместен информацискиот систем.

Евидентирање на инциденти

Член 21

Во Правилата за пријавување, реакција и санирање на инциденти, Комисијата ги определува постапките кои се применуваат за повторно враќање на личните податоци и начинот на евидентирање на овластените лица кои ги извршиле операциите за повторно враќање на личните податоци, категориите на личните податоци кои се вратени и кои биле рачно внесени при враќањето.

За повторно враќање на личните податоци, Комисијата издава писмено овластување на администраторот на информацискиот систем.

Сигурносни копии

Член 22

Комисијата е одговорна за проверка на примената на Правилата за начинот на правење на сигурносна копија, архивирање и чување, како и за повторното враќање на зачуваните лични податоци.

Сигурносни копии задолжително се прават на крајот од работната седмица на начин со кој ќе се гарантира постојана можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

Пристап до документи

Член 23

Пристапот до документите е ограничен само за овластени лица на Комисијата.

За пристапувањето до документите задолжително се воспоставуватат механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

Доколку е потребен пристап на друго лице до документите тогаш се воспоставени соодветни процедури за таа цел во документацијата за техничките и организациските мерки.

Правило „чисто биро“

Член 24

Комисијата задолжително го применува правилото „чисто биро“ при обработката на личните податоци содржани во документите за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Чување на документи

Член 25

Чувањето на документите се врши на начин на кој ќе се применат соодветни механизми за попречување на секое неовластено отворање.

Уништување на документи

Член 26

Уништувањето на документите се врши со ситнење или со друг начин, при што истите повторно да не можат да бидат употребливи.

Во случај на уништување на документи комисиски се составува записник кој ги содржи сите податоци за целосна идентификација на документите како и за категориите на личните податоци содржани во истите.

Начин на чување на документите

Член 27

Плакарите (орманите), картотеките или другата опрема за чување на документи се сместени во простории заклучени со соодветни заштитни механизми. Просториите се заклучени и за периодот кога документите не се обработуваат од овластените лица.

Копирање или умножување на документите

Член 28

Копирањето или умножувањето на докуметите може да се врши единствено со контрола на овластените лица на Комисијата, а уништувањето на копиите или умножените документи треба да се изврши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.

Пренесување на документи

Член 29

Во случај на физички пренос на документите, Комисијата задолжително презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои се пренесуваат.

Влегување во сила

Член 30

Со денот на донесување на оваа одлука престанува да важи Одлуката за вилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци бр.03-2876/1 од 09.11.2011.

Оваа одлука влегува во сила со денот на нејзиното донесување и истата ќе се објави на огласната табла на Комисијата.

Број 03-645/1
Скопје 10.06.2019 година

Комисија за хартии од вредност на
Република Северна Македонија
Претседател
Mr.Sc. Nora Aliti с.р.

Прилог - Изјава за обезбедување тајност и заштита на обработката на личните податоци

Врз основа на одредбите од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015, 99/2016 и 64/2018) и член 14 став 4 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Северна Македонија” бр. 38/09 и 158/10), на _____ година, ја давам следната

И З Ј А В А
за обезбедување тајност и заштита на обработката на личните податоци

Јас долупотпишаниот/ната, _____ (име и презиме), _____ (работно место), во _____
(организациска единица) во Комисијата за хартии од вредност на Република Северна Македонија, согласно со Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Северна Македонија” бр. 38/09 и 158/10) и документацијата за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци во Комисијата за хартии од вредност на Република Северна Македонија, се обврзувам дека:

- ќе ги почитувам начелата за заштита на личните податоци;
- ќе ги применувам техничките и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци и ќе ги чувам како доверливи личните податоци, како и мерките за нивна заштита;
- ќе вршам обработка на личните податоци согласно упатствата добиени од Комисијата за хартии од вредност на Република Северна Македонија;
- на трети лица надвор од Комисијата за хартии од вредност на Република Северна Македонија и на други лица од Комисијата за хартии од вредност на Република Северна Македонија нема да издавам каков било податок од збирките на лични податоци или каков било друг личен податок кој ми е достапен и кој сум го дознал/а или ќе го дознаам при вршењето на работата, освен ако со закон не е предвидено поинаку.

Потпис,

_____