Врз основа на член 24 став (1) точка 10) од Статутот на Регулаторна комисија за енергетика и водни услуги на Република Северна Македонија бр.01-391/2 од 26 август 2011 година и бр.01-374/6 од 19 март 2019 година и член 6 од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр.122/20), Регулаторната комисија за енергетика и водни услуги на Република Северна Македонија на седницата одржана на 30 август 2021 година донесе

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

Предмет
Член 1

Со овој правилник се пропишуваат техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци што ги применува Регулаторната комисија за енергетика за енергетика и водни услуги на Република Северна Македонија (во понатамошниот текст: Регулаторната комисија за енергетика).

Стандарди на тајност и заштита
Член 2

Регулаторната комисија за енергетика 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:

- стандардно и
- високо ниво.

Чување и евиденција
Член 3

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

Обем на примена
Член 4

Одредбите од овој Правилник се применуваат 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

Регулаторната комисија за енергетика треба да обезбеди соодветни технички мерки за тајност и заштита на обработката на личните податоци и тоа:

1. единствено корисничко име;
2. лозинка креирана од секое овластено лице, составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;
3. корисничко име и лозинка која овозможува пристап на овластеното лице до информацискиот систем во целина, на поединечни апликации и/или поединечни збирки на лични податоци потребни за извршување на неговата работа;
4. автоматизирано одјавување од информацискиот систем после изминување на определен период на неактивност (не подолго од 15 минути) и за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;
5. автоматизирано отфрлање од информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на овластеното лице дека треба да се побара инструкција од администраторот на информацискиот систем;

6. инсталирана хардверска/софтверска заштитна мрежна бариера (“firewall”) или рутер 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 системот;
7. ефективна и сигурна анти-вирусна и анти-спајвер заштита на информацискиот систем, која постојано ќе се ажурира заради превентива од непознати и непланирани закани од нови вируси и спајвери;
8. ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и
9. приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

Организациски мерки

Член 6

(1) Регулаторната комисија за енергетика треба да обезбеди соодветни организациски мерки за тајност и заштита на обработката на личните податоци и тоа:
1. ограничен пристап или идентификација за пристап до личните податоци;
2. 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;
3. уништување на документи по истекот на рокот за нивно чување;
4. мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема кадешто се собираат, обработуваат и чуваат личните податоци и
5. 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 Регулаторната комисија за енергетика, 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 понатамошен пристап

(3) Известувањето од ставот (2) на овој член се врши писмено, при било кои други промени во работниот статус или статусот на ангажирањето на овластеното лице што има влијание врз нивото на дозволениот пристап до информацискиот систем.

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 Регулаторната комисија за енергетика.

(2) Физички пристап до просторијата во која се сместени серверите имаат само лица кои се посебно овластени.

(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 Регулаторната комисија за енергетика.

(6) Во случајот од ставот (5) на овој член, меѓусебните права и обврски на Регулаторната комисија за енергетика 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 линни податоци
Член 8

Регулаторната комисија за енергетика овластува офицер за заштита на пични податоци кој ќе биде одговорен за координација и контрола на постапките и упатствата утврдени со техничките и организациските мерки за обезбедување на тајноста и ззштитата на обработката на личните податоци.

Информирање за заштитата на личните податоци
Член 9

(1) Лицата кои се вработуваат или ангажираат во Регулаторната комисија за енергетика, 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 Регулаторната комисија за енергетика во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.
(3) Регулаторната комисија за енергетика 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 Регулаторната комисија за енергетика, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци, која е дадена во Прилог и е составен дел на овој правилник.
(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 Регулаторната комисија за енергетика, 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 Регулаторната комисија за енергетика.
(7) Регулаторната комисија за енергетика 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, Регулаторната комисија за енергетика ги дефинира и утврдува во Правилникот за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.
(2) Офицерот за заштита на личните податоци во Регулаторната комисија за енергетика задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.
(3) Во извештајот од ставот (2) на овој член треба да се содржани констатираните неправилности 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, Регулаторната комисија за енергетика ги дефинира и утврдува во Правилникот за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.

(2) Регулаторната комисија за енергетика 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.

Евидентирање на инциденти

Член 12

Во Правилник за начинот на управување со инциденти, Регулаторната комисија за енергетика го определува начинот на евидентирање на секој инцидент, времето кога се појавил, овластеното лице кое го пријавило, на кого е пријавен и мерките кои се преземени за негово санирање.

Идентификација и проверка

Член 13

(1) Регулаторната комисија за енергетика задолжително води евиденција за овластените лица кои имаат авторизирани 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, Регулаторната комисија за енергетика 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.

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) Регулаторната комисија за енергетика 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) Во евиденцијата на овластените лица утврдена во член 12 став (1) на овој правилник се внесуваат и нивоата на авторизиран пристап за секое овластено лице.
(4) Администраторот на информацискиот систем кој е овластен согласно Правилникот 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 во согласност со критериумите кои се утврдени од страна на Регулаторната комисија за енергетика.

Управување со медиуми

Член 15

(1) Со медиумите треба да се овозможи идентификација и евидентирање на категориите на лични податоци и истите треба да се чуваат на локација до која пристап имаат само овластени лица утврдени со овој Правилник.
(2) Пренесувањето на медиумите надвор од работните простории се врши само со претходно писмено овластување од страна на Претседателот на Регулаторната комисија за енергетика.
(3) Регулаторната воспоставува систем за евидентирање на медиумите кои се примаат со цел да овозможи директна или индиректна идентификација на видот на медиумот кој е примен, датум и време на примање, испраќач, број на медиуми кои се примени, вид на документ кој е снимен на медиумот, начин на испраќање на медиумот, име и презиме на лицето овластено за прием на медиумот.
(4) Одредбите од ставот (3) на овој член се применуваат и за евидентирање на медиумите кои се испраќаат од страна на Регулаторната комисија за енергетика.
(5) За пренесените медиуми надвор од работните простории на Регулаторната комисија за енергетика, се преземаат неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив. Медиумите можат да се пренесуваат надвор од

работните простории само со претходно писмено овластување од страна на Претседателот на Регулаторната комисија за енергетика и ако личните податоци се криптирани или ако се заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи, при што само администраторот на информацискиот систем може да ги декриптира или лице овластено од него.

Уништување, бришење или чистење на медиумот

Член 16

(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 17

Регулаторната комисија за енергетика 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.

Евиденција на авторизираниот пристап

Член 18

(1) Регулаторната комисија за енергетика 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.
(2) Во евиденцијата од ставот (1) 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.
(3) Операциите кои овозможуваат евидентирање на податоците од ставовите (1) и (2) на овој член се контролираат од страна на офицерот за заштита на личните податоци и истите не може да се деактивираат.
(4) Евиденцијата од ставот (1) на овој член се чува најмалку пет години.
(5) Офицерот за заштита на личните податоци врши периодична проверка на податоците од ставовите (1) и (2) на овој член, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

Контрола на физички пристап

Член 19

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

Евидентирање на инциденти

Член 20

(1) Во Правилникот за начинот на управување со инциденти, Регулаторната комисија за енергетика 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.

(2) За повторно враќање на личните податоци, Регулаторната комисија за енергетика издава писмено овластување на овластените лица за да ги извршат операциите за враќање на податоците.

Сигурносни копии

Член 21

(1) Регулаторната комисија за енергетика 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.

(2) Сигурносни копии задолжително се прават секој работен ден и на крајот од работната седмица, а по потреба и секој последен работен ден во месецот.

(3) Сигурносните копии задолжително се прават 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 документите

Член 22

(1) Пристапот до документите е ограничен само за овластени лица на Регулаторната комисија за енергетика.

(2) За пристапувањето до документите задолжително се воспоставуваат механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

(3) 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 23

Регулаторната комисија за енергетика 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 24

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

Уништување на документи

Член 25

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

(2) Во случајот од ставот (1) на овој член 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 26

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 27

(1) Копирањето или умножувањето на документите може да се врши единствено со контрола на овластени лица определени со претходно писмено овластување од страна на Регулаторната комисија за енергетика.
(2) Уништувањето на копиите или умножените документи се врши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.

Пренесување на документи

Член 28

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

Преодна одредба

Член 29

Со денот на влегувањето во сила на овој правилник престанува да важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци бр. 01-3102/1 од 27 септември 2019 година.

Влегување во сила

Член 30

Овој правилник влегува во сила со денот на донесувањето, а ќе се објави на веб страницата на Регулаторната комисија за енергетика и водни услуги на Република Северна Македонија.

бр. 01-1600/1
30 август 2021 година

ПРЕТСЕДАТЕЛ на
Регулаторна комисија за енергетика и водни услуги
на Република Северна Македонија
Марко Бислимоски

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 42/2020) и член 31 став (4) од Правилникот за безбедност на обработката на личните податоци (Службен весник на РСМ бр. 122/2020). на_____година, ја давам следната

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

Јас долупотпишаниот/ната,_____(име и презиме),
_____(работно место),
во_____
(организациска единица) во Регулаторната комисија за енергетика, согласно со Правилникот за безбедност на обработката на личните податоци и документацијата за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци во Регулаторната комисија за енергетика, 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 Регулаторната комисија за енергетика;
- на трети лица надвор од Регулаторната комисија за енергетика и на други лица од Регулаторната комисија за енергетика 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,

О Б Р А З Л О Ж Е Н И Е

Врз основа на Статутот на Регулаторна комисија за енергетика и водни услуги на Република Северна Македонија и Правилникот за безбедност на обработката на личните податоци (Службен весник на РСМ бр.122/2020) а согласно Законот за заштита на личните податоци (Службен весник на РСМ бр. 42/2020), Регулаторната комисија за енергетика и водни услуги на Република Северна Македонија (во понатамошниот текст: РКЕ) пристапи кон изработка на Правилник за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

Со овој Правилник се пропишуваат техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци што ги применува РКЕ.

Изработката на овој правилник е согласно новиот Законот за заштита на личните податоци во насока на усогласување со истиот, при што РКЕ во својство на контролор има обврска да ги исполнува обврските кои произлегуваат од него.

Со денот на влегувањето во сила на овој Правилник престанува да важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци бр. 01-3102/1 од 27 септември 2019 година.

РКЕ на седницата одржана на 30 август 2021 година донесе Правилник за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.