РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
УСТАВЕН СУД НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ, ЗАШТИТА И БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО УСТАВНИОТ СУД НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Скопје, јули 2023 година

Врз основа на член 89 алинеја 1 од Деловникот на Уставниот суд на Република Северна Македонија („Службен весник на Република Македонија“ бр.70/1992 и „Службен весник на Република Северна Македонија“ бр.202/2019, 256/2020, и 65/2021), член 28 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија„ бр. 42/20 и 294/21) и член 6 од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија„ бр.122/20) Уставниот суд на Република Северна Македонија, на седницата одржана на 18 јули 2023 година, донесе

ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ, ЗАШТИТА И БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. ОПШТИ ОДРЕДБИ

Член 1

Со овој правилник се пропишуваат техничките и организациските мерки кои ги применува Уставниот суд на Република Северна Македонија (во натамошниот текст: Судот) заради обезбедување тајност, заштита и безбедност на личните податоци со кои располага и ги обработува Судот.

Член 2

Одредбите од овој правилник се применуваат за:

-целосно и делумно автоматизирана обработка на личните податоци;

-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.

Член 3

Земајќи ги во предвид природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста за правата и слободите на физичките лица, контролорот е должен да примени соодветно ниво на технички и организациски мерки кое ќе биде пропорционално и на активностите за обработка на личните податоци.

Техничките и организациските мерки од ставот (1) на овој член се класифицираат во две нивоа:

-стандардно;
-високо ниво.

Член 4

Судот е одговорен за усогласеноста во однос на нивото на мерки за безбедност на обработката на личните податоци кои ќе ги примени во согласност со член 3 од овој Правилник, при што треба да обезбеди соодветно ниво на безбедност на личните податоци, вклучувајќи заштита од неовластена или незаконска обработка како и заштита од нивно случајно губење, уништување или оштетување.

Судот ја демонстрира примената на мерките според барањата утврдени од ставот 1 на овој член вклучувајќи ги причините и основите за изборот на примената на стандардното, односно високото ниво на класификација.

II. ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Евидентирање и чување на документацијата за софтверски програми

Член 5

Судот врши евидентирање и ја чува целокупната документација за софтверските програми за обработка на личните податоци и сите нивни промени.

Одржување на информатичкиот систем

Член 6

Вработените во Судот кои ги вршат работите од областа на информатичко-комуникациската технологија се должни да вршат одржување на информатичкиот систем во Судот, согласно документацијата на Судот за техничките и организациските мерки.

III. СТАНДАРДНО НИВО

Документација за технички и организациски мерки на стандардно ниво

Член 7

Судот во Политиката за системот за заштита на личните податоци ги утврдува и начелата за безбедност и заштита на личните податоци.

Врз основа на Политиката за системот за заштита на личните податоци, Судот донесува подетални политики и процедури во кои се опишани техничките и организациските мерки за овластените лица кои имаат пристап до личните податоци и до информатичкиот систем и информатичката инфраструктура.

Документацијата од ставот (2) Судот ја менува и дополнува кога ќе се направат промени во информатичкиот систем и информатичката инфраструктура, а најмалку еднаш годишно врши нејзино оценување, евалуација и ажурирање.

1. Технички мерки

Автентикација на овластени лица

Член 8

Во Судот се обезбедува најава во информатичкиот систем преку единствен идентикатор кој се поврзува само со едно овластено лице.

Во согласност со ставот (1) од овој член единствениот идентификатор Судот може да го обезбеди преку:

- информација која единствено овластеното лице ја знае (на пример: единствено корисничко име и лозинка за секое овластено лице, при што лозинката треба да биде составена од комбинација на најмалку осум алфанумерички карактери букви (мали и големи), симболи, броеви и интерпукциски знаци;

Судот задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и информатичкиот систем, како и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

Кога проверката се врши врз основа на корисничко име и лозинка, Судот секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите, при што лозинките задолжително автоматски се менуваат по изминат определен временски период врз основа на анализата на ризикот кој не може да биде подолг од три месеци.

Обезбедување на опремата на која се врши обработка на личните податоци

Член 9

Судот е должен да обезбеди примена на технички мерки со кои се обезбедува опремата на која се врши обработка на личните податоци и тоа:

- автоматизирано одјавување од информатичкиот систем после изминување на определен период на неактивност (не подолго од 15 минути). За повторно активирање на системот, Судот треба да обезбеди дека

овластените лица пристапуваат со примена на автентикацијата во согласност со член 8 од овој правилник;

- во случај на одреден број на неуспешни обиди за најавување на информатичкиот систем, кои се во спротивност со политиките за автентикација на контролорот, треба да се обезбеди автоматизирано отфрлање од информатичкиот систем. Бројот на неуспешни обиди Судот го определува соодветно на ризикот и природата на работата и работните процеси во однос на обработката на личните податоци, но не повеќе од пет последователни неуспешни обиди;

- инсталиран заштитен ѕид (firewall) и ограничување на овластените порти за комуникација на оние што се строго неопходни за правилна работа на софтверските програми инсталирани на работните станици на Судот;

- редовно ажуриран антивирусен софтвер и дефинирана политика за редовни ажурирања на софтверските програми;

- конфигурирани софтверски програми така што безбедносните ажурирања да се вршат автоматски;

- зачувување на податоците на корисниците на серверите на Судот за кои редовно се прави сигурносна копија;

- ограничување на опцијата за приклучување на преносливите медиуми (УСБ, надворешни хард дискови и сл.) кон системите со примарна важност;

- исклучен автоматски режим на работа за преносливите медиуми (Disable autorun for removable media);

- алатките за далечинска администрација мора да бидат нагодени на начин што претходно задолжително треба да обезбедат согласност од корисникот (овластеното лице) на работната станица пред каква било интервенција на самата работна станица;

- нагодување на информатичкиот систем кое ќе обезбеди дека корисникот (овластеното лице) на работната станица може да забележи дали се врши далечинска администрација, како и за тоа кога истата завршила (на пример со прикажување на порака на екранот дека далечинската администрација завршила); и

- приклучување на информатичкиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

Покрај мерките од ставот (1) на овој член, врз основа на спроведената анализа на ризик, доколку се утврди за потребно, Судот ги применува и следните мерки:

- забрана на работа со преземени софтверски програми кои не доаѓаат од безбедни извори;

- ограничување на употребата на софтверски програми што бараат администраторски права;

- бришење на податоците што се наоѓаат на работна станица која треба да се предаде;

- во случај работната станица да биде компромитирана, задолжително испитување и по можност пронаоѓање на изворот, како и каква било трага од упадот во информатичкиот систем на Судот, со цел откривање дали се загрозени и други елементи;

- безбедносен надзор на софтверот и хардверот што се користи во системот на Судот, вклучувајќи и редовно следење на тимот за брза реакција (MKD-CIRT) во однос на неговите предупредувања и совети за ранливости откриени во софтверот и хардверот;

- ажурирање на софтверските програми кога се идентификуваат и ги коригираат критичните недостатоци;

- инсталирање на ажурирања на оперативните системи со автоматска верификација согласно проценатa на ризик, а најмалку еднаш неделно; и

- подигнување на нивото на свесност во однос на тоа, на што овластените лица треба да се посветат и податоци за контакт на лицата што треба да ги контактираат во случај на инцидент или појава на необичен настан што влијае на информациите и комуникацијата на системите на Судот.

Сегрегација на должности и одговорности

Член 10

Судот ги утврдува овластените лица кои треба да имаат пристап до информатичкиот систем при што обезбедува јасна поделба на должностите и одговорностите според правилото „потребно е да знае“, односно дека овластеното лице ќе има пристап само до оние лични податоци за кои има неопходна потреба заради извршување на своите должности.

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

Судот врши проверка и ажурирање на привилегиите за пристап до информатичкиот систем на овластените лица. Проверката се врши за периоди

кои се определуваат врз основа на анализата на ризикот, а најмалку квартално.

Контрола на пристап до информатичкиот систем

Член 11

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

Судот 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 на информатичкиот систем (Советник на Судот за ИТ) кој е овластен од Судот, 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 Судот.

Евидентирање на инциденти

Член 12

Начинот на евидентирање на секој инцидент, времето кога се појавил, корисникот кој го пријавил, на кого е пријавен и преземените мерки ќе бидат утврдени со Правилник на Судот за пријавување, реакција и санирање на инциденти.

Постапки за идентификација, проверка и водење на евиденција за овластените лица кои имаат авторизиран пристап до документите и информатичкиот систем

Член 13

Судот задолжително воспоставува постапки за идентификација и проверка на авторизираниот пристап до документите и информатичкиот систем.

Кога проверката од ставот 1 од овој член се врши врз основа на корисничко име и лозинка Судот секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите.

Лозинките автоматски се менуваат во период од три месеци, се чуваат заштитени со соодветни методи, така што истите нема да бидат разбирливи додека се валидни.

Член 14

Судот задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и информатичкиот систем.

Евиденцијата од ставот (1) на овој член треба да ги содржи особено следните податоци: име и презиме на овластеното лице, работната станица од каде се пристапува до информатичкиот 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 информатичкиот систем.

Во евиденцијата од ставот (1) на овој член се внесуваат и податоци за идентификување на информатичкиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво на авторизација.

Операциите кои овозможуваат евидентирање на податоците од ставовите (2) и (3) на овој член треба да бидат контролирани од страна на офицерот за заштита на личните податоци и од друго овластено лице од Судот кое ги има потребните знаења и вештини, но нема администраторски привилегии и истите задолжително треба да бидат нагодени на таков начин што нема да може да се деактивираат. Во однос на евиденцијата на податоците за пристап, Судот може да користи и алатки кои податоците ги генерираат во едноставна и лесно разбирлива форма за читање.

Евиденцијата од ставот (1) на овој член се чува најмалку пет години.

Судот обезбедува дека овластените лица за управување со системот за евиденција за пристап до информатичкиот систем го известуваат раководството за која било аномалија или безбедносен инцидент, веднаш, а најдоцна во рок од 12 часа од моментот на инцидентот.

Судот ја известува Агенцијата за заштита на личните податоци за секое нарушување на безбедноста на личните податоци, а доколку постои веројатност да предизвика висок ризик за правата и слободите на физичките лица, и субјектите на личните податоци за да можат да ги ограничат последиците од нарушувањето на безбедноста.

Заштита на внатрешната мрежа

Член 15

Судот обезбедува заштита на својата внатрешна мрежа преку овозможување само на неопходните мрежни функции потребни за обработка на личните податоци, а особено преку:

- ограничување на пристапот до интернет со блокирање на несуштински услуги и сервиси (VoIP, peer to peer, итн.);

- управување со Wi-Fi мрежата кое опфаќа користење на најсовремените методи на криптирање (на пример: WPA2 или WPA2-PSK и со употреба на комплексна лозинка која на определен временски период се менува);

- Wi-Fi мрежата која е отворена за употреба на лица кои не се овластени (на пример надворешни посетители) задолжително да биде одвоена од внатрешната мрежа;

- во случај на далечински пристап, задолжително воспоставување на VPN конекција, со задолжителна автентикација на овластеното лице (на пример: паметна картичка, уред за генерирање лозинка за еднократна употреба – OTP и слично);

- обезбедување ниту еден административен панел за управување со содржина и нагодување на системот да не биде директно достапен преку интернет (далечинското одржување задолжително да се изврши преку VPN); и

- ограничување на мрежниот сообраќај со филтрирање на влезниот/појдовниот сообраќај на опрема со заштитен sид, прокси сервери, итн (на пример: ако веб серверот користи HTTPS, да се обезбеди влезниот сообраќај да биде преку портата 443 и со блокирање на сите други пристапи).

Судот врз основа на анализата на ризикот, покрај мерките наведени во ставот (1) од овој член, може да примени и други мерки со кои ќе ја зајакне заштитата на својата внатрешна мрежа.

Обезбедување на серверите

Член 16

Судот согласно анализата на ризик е должен на врвот на својата листа од аспект на примената на технички и организациски мерки да ги има своите сервери на кои се централизира обработката на голема количина на лични податоци. При тоа Судот ги применува особено (најмалку) следните мерки:

- единствено овластени лица кои ги имаат потребните знаења може да имаат пристап до алатките и административни панели на серверите;

- примена на овластувања со помалку привилегии за лицата кои не се администратори на информатичкиот систем (вообичаени операции за стандардни корисници);

- примена на посебна политика за креирање и употреба на лозинките за администраторите на информатичкиот систем (на пример: промена на лозинките по секое заминување на администраторот, употреба на повеќе факторска лозинка...);

- инсталирање на сите важни ажурирања (updates) за оперативните системи и за апликациите во временски интервал врз основа на анализата на ризикот, но не подолго од седмично ажурирање со нагодување на системот за автоматско ажурирање (auto update);

- правење на сигурносни копии и нивна редовна проверка; и

- примена на TLS протокол (со замена на SSL13) или друг протокол што обезбедува шифрирање и автентикација, како минимум за каква било размена на податоци преку интернет и потврда на нејзината соодветна примена преку соодветни алатки.

Во случај кога се врши администрирање на базите на податоци, Судот ги применува најмалку следните мерки:

- употреба на персонализирани профили за пристап до базите на податоци и креирање на посебно корисничко име за секоја апликација (specific account for each application); и

- примена на мерки против напади преку инјектирање на SQL код, скрипти и слично.

Обезбедување на веб-страницата на Судот

Член 17

Судот кој има своја веб-страница треба да примени технички мерки со кои ќе го гарантира точниот идентитет на страницата (pharming prevention), како и доверливоста на информациите што ги испраќа или ги собира преку веб-страницата, и тоа особено преку следните мерки:

- имплементација на криптографски протокол (TLS заменувајќи го SSL) на сите веб страници на Судот (ако има повеќе од една), користејќи ја

единствено најновата верзија и со проверка на неговата правилна имплементација;

- задолжителна употреба на криптографски протокол (TLS) за сите страници од веб-страницата, вклучително и формулари за собирање лични податоци или овозможување автентикација на корисникот и на оние на кои се прикажани или се пренесуваат лични податоци кои не се јавно достапни;

- ограничување на портите за комуникација на оние кои се строго потребни за правилно функционирање на инсталираните апликации. Ако веб серверот прифаќа само врски со HTTPS протокол, само IP мрежен сообраќај кој влегува преку портата 443 е дозволен, а сите други пристапни порти мора да бидат блокирани;

- обезбедување дека само овластени лица ќе можат да имаат пристап до алатките и административните интерфејси, при што особено да се ограничи употребата да биде достапна само до овластените лица со администраторски привилегии кои се дел од тимот одговорен за информатичката технологија и само за административни активности што се неопходни; и

- ако се користат колачиња што не се потребни од услугата, Судот обезбедува претходна согласност од интернет корисникот откако ќе го извести корисникот, а пред да се депонира колачето;

Судот кој има своја веб-страница не треба да применува практики кои го зголемуваат ризикот од можна злоупотреба, несакана (случајна) или намерна неовластена обработка на личните податоци, а особено:

- да не пренесува лични податоци преку URL без примена на протокол за криптирање (на пример идентификатори или лозинки);

- користење на небезбедни услуги;

- употреба на сервери кои хостираат бази на податоци или сервери како работни станици, особено не за пребарување на веб-страници, пристап до електронски пораки и слично;

- поставување на базите на податоци на сервери кои се директно достапни преку интернет; и

- споделување и употреба на корисничките сметки (user accounts) помеѓу две или повеќе овластени лица.

Обврски и одговорности на администраторот на информатичкиот систем и на овластените лица

Член 18

Судот врз основа на спроведената анализа на ризик, ги определува обврските и одговорностите на администраторот на информатичкиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема, применувајќи ги најмалку мерките кои се предвидени со овој правилник.

Судот задолжително врши периодична контрола над работата на администраторот на информатичкиот систем и изработува извештај за извршената контрола.

Во извештајот од ставот (2) се наведуваат констатираните неправилности (доколку ги има) и предложените мерки за отстранување на тие неправилности.

Судот задолжително ги информира администраторот и овластените лица од ставот (1) на овој член за документацијата за технички и организациски мерки која се однесува на извршувањето на нивните обврски и одговорности.

Управување со преносливи медиуми

Член 19

Преносливите медиуми на кои се врши обработка на личните податоци Судот обезбедува дека се чуваат на локација до која пристап имаат само овластени лица утврдени од негова страна.

Пренесувањето на медиумите од ставот (1) на овој член надвор од работните простории се врши само со претходно овластување од страна на Судот.

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.

Уништувањето на медиумот се врши на начин кој ќе гарантира дека податоците кои биле снимени на него не можат повторно да бидат реконструирани (на пример: со механичко разделување на неговите составни делови).

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

За случаите од ставовите (4) и (5) на овој член Судот обезбедува информациска трага (на пример: записник), која ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци кои биле снимени на истиот.

Член 20

Постапките и процедурите за уништување како и за бришење или чистењето на медиумот ќе бидат определени со Правилник за начинот на уништување на документите.

Физичка безбедност

Член 21

Серверите на кои е инсталиран софтверот кој содржи лични податоци е физички лоциран во службените простории на Судот во посебна просторија (сервер-сала) заедно со останатите сервери дел од информатичко-комуникацискиот систем на Судот, до која пристап имаат само Советниците на судот кои ги вршат работите од областа на информатичко-комуникацискатa технологија, кои се задолжени за одржување на информатичкиот систем на Судот.

Доколку е потребен пристап на друго лице до просторијата во кои се наоѓаат серверите, тогаш тоа лице треба да биде придружувано и надгледувано од вработените во Судот од ставот 1 на овој член.

За просторијата во која се наоѓаат серверите се превземаат мерки за заштита од потенцијални закани како што се кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електро магнетно зрачење.

Контрола на информацискиот систем и информатичката инфраструктура

Член 22

Во документацијата за технички и организациски мерки утврдена во членот 8 од овој правилник, задолжително треба да се содржани постапките за овластување на офицерот за заштита на личните податоци, за вршење периодични контроли, заради следење на усогласеноста на работењето на контролорот со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

Информатичкиот систем и информатичката инфраструктура на Судот задолжително подлежат на годишна внатрешна контрола со цел да се провери дали постапките и упатствата содржани во правилата и политиките за

безбедност на личните податоци се применуваат и се во согласност со прописите за заштита на личните податоци.

2. Организациски мерки

Организациски мерки за безбедност на личните податоци (минимален стандард)

Член 23

Пристап до личните податоци на сите вработени во Судот имаат само вработените лица во Судот овластени за внесување, измена или бришење на лични податоци во софтверот, како и раководни лица кои се овластени да дадат одобрување на внесувањето,измените или бришењето на личните податоци во софтверот.

Пристап до софтверот за пресметка на платите на вработените во Судот со личните податоци од вработените имаат само вработените лица кои вршат работни задачи во врска со пресметка на плати на вработените согласно Правилникот за внатрешна организација и систематизација на работите и задачите на Судот.

Пристап за обработка на личните податоци на странките, во врска со поднесените иницијативи или барања до Судот имаат само вработените во Судот кои вршат работни задачи согласно Правилникот за внатрешна организација и систематизација на работите и задачите на Судот.

Личните податоци на вработените во Судот и личните податоци на странките и третите лица во постапките кои се водат пред Судот, во секое време се чуваат во заклучени шкафови и пристап до нив имаат вработените кои вршат работни задачи во врска со водење на тековните работи согласно Правилникот за внатрешна организација и систематизација на работите и задачите на Судот.

Судот е должен да обезбеди соодветни организациски мерки за безбедност на личните податоци врз основа на резултатите од анализата на спроведениот ризик, а особено да обезбеди:

- Ограничен пристап со 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; и

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

Вработеното лице кое ги врши работите за човечки ресурси во Судот, го известува администраторот на информатичкиот систем за вработувањето или ангажирањето на секое овластено лице со право на пристап до информатичкиот 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 од ставот (6) на овој член се врши и при било кои други промени во работниот статус или статусот на ангажирањето на овластеното лице што има влијание врз нивото на дозволениот пристап до информатичкиот систем.

Информирање и едуцирање за заштитата на личните податоци

Член 24

Лицата кои се вработуваат или се ангажираат во Судот, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерк на Судот.

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

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

Лицата кои се вработуваат или се ангажираат во Судот, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.

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 Судот, освен ако со закон поинаку не е уредено и ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита.

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

Судот задолжително врши континуирано информирање и едуцирање на раководството и овластените лица за непосредните обврски и одговорности за заштита на личните податоци.

Пристап до документите

Член 25

Пристапот до документите треба биде ограничен само за овластени лица во Судот.

За пристапувањето до документите задолжително треба да се воспостават 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 треба да бидат воспоставени соодветни процедури за таа цел во документацијата за техничките и организациските мерки.

Правило „чисто биро“

Член 26

Вработените во Судот 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 27

Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отворање.

Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот (1) на овој член, Судот треба да примени други мерки кои што ќе го спречат секој неовластен пристап до документите.

Ако документите не се чуваат заштитени на начин определен во ставовите (1) и (2) на овој член, тогаш Судот треба да ги примени сите мерки за

нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Уништување на документи

Член 28

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

Во случајот од ставот (1) на овој член комисиски се составува записник кој ги содржи сите податоци за целосна идентификација на документот како и за категориите на личните податоци содржани во истиот.

Начин на чување на документите

Член 29

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

Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки за да се спречи секој неовластен пристап до документите.

IV. ВИСОКО НИВО

1. Технички мерки

Дополнителни мерки

Член 30

Судот врз основа на анализата на ризикот воведува и применува дополнителни мерки за безбедност на личните податоци со кои ќе демонстрира дополнителна усогласеност со прописите и добрите практики за заштита на личните податоци.

Тестирање на информатичкиот систем

Член 31

Судот задолжително врши тестирање на информатичкиот систем пред неговото имплементирање или по извршените промени со цел да се провери

дали системот обезбедува безбедност на личните податоци согласно со прописите за заштита на личните податоци.

Тестирањето од став (1) на овој член се врши преку обработка на документи кои содржат имагинарни лични податоци.

2. Организациски мерки

Копирање и умножување на документите

Член 45

Копирањето или умножувањето на документите може да се врши единствено од страна на овластени лица определени со процедура од страна на Судот во која задолжително се утврдуваат мерките и начинот на копирањето и умножувањето на документите.

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 46

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

V. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 47

Овој правилник влегува во сила од денот на неговото донесување и истиот ќе биде објавен на веб страната на Судот.

Су.бр. 1110/23
20 јули 2023 година
С к о п ј е

ПРЕТСЕДАТЕЛ
на Уставниот суд на
Република Северна Македонија,
Добрила Кацарска