



Република Северна Македонија
Republika e Maqedonisë së Veriut
Национална установа Кинотека на
Република Северна Македонија
Institucioni Nacional Kinoteka e
Republikës së Maqedonisë së Veriut

Бр.-Nr. 01-861/1
25.8 2022 год.-viti
Gronje-Shkup

**ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИ МЕРКИ ЗА
ОБЕЗБЕДУВАЊЕ ТАЈНОСТ, ЗАШТИТА И БЕЗБЕДНОСТ НА
ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО
НУ КИНОТЕКА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА**

Содржина

Општи одредби	3
Основни начела за правична и законска обработка	3
Законитост на обработка	4
Систем за заштита на личните податоци	7
Физичка безбедност.....	10
Мрежно поврзување и комуникација	11
Интернет сервиси	12
Обезбедување на серверите и персоналните компјутери на која се врши обработка на личните податоци	14
Управување со корисници.....	14
Управување со лозинки	16
Систем за мониторинг и контрола	17
План за континуитет и сигурносни копии	17
Енкрипција	19
Обезбедување на преносливите медиуми.....	19
Справување со инциденти	20
Управување со обработувачи	20
Чување на документација – правило на чисто биро.....	21
Рокови за чување на личните податоци	22
Тестирање (високо ниво).....	22
Периодична контрола.....	22
Завршни одредби.....	23

Врз основа на Законот за заштита на лични податоци („Сл. Весник бр. 42/20) и Правилникот за безбедност на обработката на личните податоци („Сл. Весник бр. 122/2020) НУ Кинотека на Република Северна Македонија донесе

**ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ,
ЗАШТИТА И БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ
ВО НУ КИНОТЕКА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА**

Општи одредби

Член 1

Со правилникот за техничките и организациски мерки за обезбедување тајност, заштита и безбедност на обработката на личните податоци (во понатамошниот текст: Правилникот) на НУ Кинотека на Република Северна Македонија (во понатамошниот текст: Кинотека) се пропишуваат техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

Член 2

Правилникот ги дефинира принципите и определува рамка на мерки и одговорности во делот на заштитата на личните податоци во фазите на нивното прибирање, чување, обработка, пренос, архивирање и уништување во согласност со Законот за заштита на личните податоци (Закон за ЗЗЛП) и соодветните правилници на Агенцијата за заштита на личните податоци.

Член 3

Правилникот се применува и употребува во сите организациони делови на Кинотека а се однесува на сите вработени, ангажирани лица, практиканти и надворешни/трети лица.

Вработените со објавувањето на овој Правилник се сметаат за запознаени и свесни за обврските дефинирани во истиот.

Член 4

Одредбите од овој Правилник се применуваат за:

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

Основни начела за правична и законска обработка

Член 5

Согласно Законот за заштита на личните податоци (Закон за ЗЛП) и Европската регулатива за заштита на личните податоци (General Data Protection Regulation GDPR) воспоставени се следниче принципи на заштита на податоците како темелни вредност:

- Личните податоци се прибираат и обработуваат со законски основ, на транспарентен начин (претходно информирање) и со почитување на правилата за обработка на сензитивните податоци (лични податоци што го откриваат расното или етничко потекло, политичката определба,

религиозни или филозофски определби, членување во синдикати и обработка на податоци за здравствената состојба или сексуалниот живот).

- Личните податоци се обработуваат согласно со закон, во доволна мера и на транспарентен начин во однос на субјектот на личните податоци („законитост, правичност и транспарентност“),
- Личните податоци се собираат за конкретни, јасни и легитимни цели и нема да се обработуваат на начин што не е во согласност со тие цели.
- Личните податоци се соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат („минимален обем на податоци“),
- Личните податоци се точни и каде што е потребно ажурирани, при што ќе се преземат сите соодветни мерки за навремено бришење или коригирање на податоците што се неточни или нецелосни, имајќи ги предвид целите заради кои биле обработени („точност“),
- Личните податоци се чувани во форма која овозможува идентификација на субјектите на личните податоци, не подолго од она што е потребно за целите поради кои се обработуваат личните податоци. Личните податоци може да се чуваат подолго од нивниот рок на чување ако се обработуваат за статистички цели, подготвка на извештаи, остварување на законските обврски на Контролорот, а со применување на соодветни технички и организациски мерки согласно со овој закон, заради заштита на правата и слободите на субјектот на личните податоци („ограничување на рокот на чување“),
- Личните податоци се обработени на начин кој обезбедува соодветно ниво на безбедност на личните податоци, вклучувајќи заштита од неовластена или незаконска обработка, како и нивно случајно губење, уништување или оштетување, со примена на соодветни технички или организациски мерки („интегритет и доверливост“).
- Применети се соодветни технички и организациони мерки за заштита од неавторизирано или незаконско обработување на личните податоци и спречување на инцидентно губење, уништување или оштетување на личните податоци.
- Личните податоци нема да се пренесуваат во земја или територија надвор од Европската Унија или Европската Економска Заедница доколку таа земја или територија не обезбеди соодветно ниво на заштита на правата и слободите на субјектите во врска со обработката на личните податоци.

Член 6

За остварување на овие основни цели, Кинотека како Контролор, развива и одржува систем на интерни контроли со соодветни организациски и технички мерки во согласност за Законот за ЗЗЛП, придржните Правилници како и релевантните најдобри практики и стандарди.

Законитост на обработка

Член 7

Согласно Законот за заштита на личните податоци, Кинотека целосно ја почитува законитоста при прибирањето и обработката на личните податоци, со исполнување на најмалку еден од следните услови:

- субјектот на лични податоци дал експлицитна и јасна согласност за обработка на неговите лични податоци за една или повеќе конкретни цели,

- обработката е потребна за исполнување на договор каде субјектот на лични податоци е договорна страна, или за да се преземат активности на барање на субјектот на лични податоци пред неговото пристапување кон договорот,
- обработката е потребна за исполнување на законска обврска на контролорот, - обработката е потребна за заштита на суштинските интереси на субјектот на лични податоци или на друго физичко лице,
- обработката е потребна за извршување на работи од јавен интерес или при вршење на јавно овластување на контролорот утврдено со закон,
- обработката е потребна за целите на легитимните интереси на контролорот или на трето лице, освен кога таквите интереси не преовладуваат над интересите или основните права и слободи на субјектот на лични податоци коишто бараат заштита на личните податоци, особено кога субјектот на личните податоци е дете.

Член 8

Кинотека го прибира и обработува ЕМБР (Единствениот Матичен Број на Граѓанинот) под следниве услови:

- ако е добиена претходно изречена согласност на субјектот на лични податоци;
- за остварување на со закон утврдени права или обврски на Контролорот или субјектот на лични податоци;
- други случаји утврдени со закон;

Кинотека ќе преземе потребни мерки ЕМБР да не е непотребно видлив и изложен при обработката, преносот и чувањето, согласно насоките за обработка содржани во Правилникот за евиденција на обработка на збирки со висок ризик.

Член 9

Кинотека како Контролот нема да прибира и обработува посебни категории на лични податоци.

По исклучок обработката на посебни категории на лични податоци ќе ја врши ако:

- е добиена изречна согласност на субјектот на личните податоци за обработка на таквите податоци, се во случај кога со закон е предвидено дека забраната за обработка на таквите податоци не може да се отстрани со согласност на субјектот на лични податоци;
- за исполнување на посебните права и обврски во областа на законот за работни односи, во обем и соодветна заштита определена со закон во таа област.
- кога е неопходно за заштита на субјектот на податоци или друго лице, ако последното има пречки што го спречуваат да даде согласност или е деловно неспособно за давање на согласност.
- обработката се однесува на податоци кои субјектот на лични податоци јавно ги објавил.

Член 10

Кинотека како Контролор целосно ги почитува правата, слободите и легитимните интереси на субјектот при прибирањето и обработката на личните податоци, согласно Законот за заштита на личните податоци:

- ✓ право на транспарентност информираност (член 16)
- ✓ право на пристап до лични податоци (член 19),
- ✓ право на исправка (член 20),
- ✓ право на бришење (член 21),
- ✓ право на ограничување на обработката (член 22),
- ✓ право на преносливост (член 23),
- ✓ право на приговор (член 24) и
- ✓ право да не биде предмет на одлука заснована единствено на автоматизирана обработка, вклучувајќи профилирање (член 25).

Член 11

Принципот на отчетност и транспарентност е фундаментален принцип на секој систем за заштита на личните податоци.

Кинотека на својот web сајт како Контролот има воспоставено Политика за приватност и јавно достапни информации за контакт со Контролорот и Офицерот за заштита на личните податоци со јасни насоки за транспарентно информирање и остварување на правата на субјектите на личните податоци согласно Законот за ЗЗЛП.

Член 12

Како Контролот во моментот на собирањето на личните податоци, на субјектот на личните податоци му ги обезбедува следните информации:

- идентитетот и контакт податоците на Контролорот и податоци за неговиот овластен претставник во Република Северна Македонија;
- контакт податоци за Офицерот за заштита на личните податоци;
- целите на обработката за коишто личните податоци се наменети, како и правната основа за обработката;
- легитимните интереси што ги спроведува контролорот или трето лице
- корисниците или категориите на корисници на личните податоци, доколку ги има;
- каде што е применливо, фактот дека контролорот има намера да пренесе лични податоци во трета земја или меѓународна организација, повикување на соодветните или прифатените заштитни мерки и начинот за добивање на копија од нив или информации каде истите се достапни.

Член 13

На барање на субјектот на личните податоци, Кинотека доставува информација до подносителот за мерките и активностите кои ги презема а врз основа на членовите од 19 до 25 од Законот за заштита на личните податоци, без непотребно одлужување во период од еден месец од денот на приемот на барањето.

Доколку е потребно овој рок може да биде продолжен за уште два месеци земајќи ги предвид сложеноста и бројот на барањата. Контролорот го информира субјектот на личните податоци за секое продолжување во рок од еден месец од денот на приемот на барањето, заедно со причината за одложувањето.

Член 14

Барањата во врска со остварување на своите права од член 19-25, субјектите на личните податоци може да ги остварат преку:

- Преку e-mail на офицерот
- Преку достава на пошта со назнака за *Офицер за заштита на лични податоци*
- Преку директна достава во Архива во централата со назнака за *Офицер за заштита на лични податоци*

Систем за заштита на личните податоци

Член 15

Безбедноста на личните податоци е прашње кое е многу пошироко од едноставна примена на соодветни технички и организациски мерки. Безбедноста е предуслов за постигнување усогласеност со сите други принципи на обработка на личните податоци.

Кинотека има воспоставено систем со организациски и технички мерки во согласност со Правилникот за безбедност на Агенцијата за заштита на личните податоци.

Безбедноста на личните податоци се обезбедува преку исполнување на следниве атрибути:

-Доверливост (анг. Confidentiality): Податокот е достапен само на оние коишто имаат овластен пристап до неа;

- Интегритет (анг. Integrity): Заштита на точноста и конзистентноста на податоците и на методите на обработка;

-Расположливост (анг. Availability): Овластените корисници имаат пристап до податоците и до другите придружни средства потребни за нејзина презентација, кога за тоа има деловна потреба;

- Неодречливост (анг. Non-Repudiation): Потврда и непорекливост на активностите поврзани со пристапот и користењето на податоците;

-Отчетност (анг. Accountability): Активностите поврзани со користењето и пристап до податоците треба да бидат еднозначно забележани и евидентирани.

Член 16

Според најновите технолошки достигнувања, трошоците за спроведување и природата, обемот, контекстот и целите на обработката, како и ризиците со различен степен на веројатност и сериозноста за правата и слободите на физичките лица, Кинотека воспоставува систем за заштита на личните податоци преку примена на соодветни технички и организациски мерки за да обезбеди ниво на безбедност соодветно на ризикот.

Систем за заштита на личните податоци ги опфаќа следниве области:

- Проценка на нивото на ризик, опфатени во Методологијата за проценка на влијание на, согласно член 39 од Законот за Заштита на личните податоци.

При утврдувањето и процената на ризикот (управување со ризик) ги зема во предвид ризиците кои се поврзани со обработката, особено од случајно или незаконско уништување, губење,

менување, неовластено откривање на личните податоци или неовластен пристап до пренесените, зачуваните или на друг начин обработени лични податоци.

- Имплементација на соодветен систем на контроли кои се поделени на
 - Физички контроли, кои служат за обезбедување на адекватна физичка сигурност на информацијата и информативните средства (сервери, мрежни уреди).

Како примери на физички контроли се употребата на уреди за непрекинато напојување (анг. UPS), чуварска служба, сензори и аларми и слични мерки за контрола на физичкиот пристап и заштита на ресурсите и средствата кои се користат за обработката, пренос и чување на личните податоци

– Технички контроли, се контроли кои се вградени во информативните средства односно апликативниот софтвер, мрежно - комуникациската опрема и придружните уреди. Техничките контроли уште се наречени и логички контроли.

– Административни контроли, вклучуваат воспоставување процедури и упатства, за овластување на корисниците (вработени, трети лица) кои имаат пристап до информативниот систем, им се овозможува потребната авторизација за извршување на своите деловни процеси и имаат јасна слика за активностите во поглед на обезбедување на посигурен информативен систем..

- Примена на принципот на заштита на личните податоци by design односно by default, согласно Член 10, III. Стандардно ниво, од Правилник за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци.

Според овој принцип соодветните технички и организациски мерки се вградени во процесот на обработка на личните податоци уште во моментот на дефинирање на средствата на обработка. Овој принцип се применува и при тековни активности и средства за обработка, за да се осигура контролорот дека ефективно се справува со целиот животен век на личните податоци коишто ги обработува.

Член 17

Земајќи ги 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 може да се класифицираат во две нивоа:

- стандардно и
- високо

Член 18

Кинотека ги применува следните нивоа на технички и организациски мерки од стандардно ниво, согласно Член 10, III. Стандардно ниво, од Правилник за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци.

- Физичка безбедност на компјутерската и другата опрема која се користи за обработка на личните податоци

- Соодветни методи за автентикација и регистрација на корисниците кои пристапуваат до компјутерскиот систем;
- Соодветни политики и правила за управување со лозинките;
- Автоматизирано одјавување на информацискиот систем после изминување на определен период од 15 минути на неактивност и за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;
- Инсталирана хардверска/софтверска заштитна мрежна бариера („анг. Firewall“) и рутерпомеѓу информацискиот систем и интернет или било која друга форма на надворешна мрежа , како заштитна мерка против недоволени или злонамерни обиди за влез или пробивање на системот;
- 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;
- Ефективна и сигурна анти-спам заштита на системот за електронска пошта , која постојано се ажурира заради превентивна заштита од спамови и други малициозни кодови;
- Приклучување на компјутерската и другата опрема на енергетска мрежа преку уред за непрекинато напојување;
- Обезбедување на соодветна локација за чување на сигурносни копии (backup) од личните податоци во заштитена форма;
- Обезбедување на локација за опоравување од катастрофа (disaster recovery location) каде се прави репликација на податоците од серверите на примарната локација, а во кој се вклучени file server, e-mail server, web server, итн.
- Процес за ефикасна детекција и справување со сигурносни инциденти;
- Управување со преносливи медиуми;

Член 19

Кинотека ги применува следните нивоа на технички и организациски мерки од високо ниво, согласно делот IV. Високо Ниво, од Правилник за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци:

- Управување со лозинки – кои се однесуваат на заштита и злоупотреба на системот за чување и користење на лозинките (password hashing), согласно член 38, IV. Високо Ниво, од Правилник за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци
- Управување со преносливи медиуми - преку користење на соодветни методи за заштита (енкрипција) кои гарантираат дека податоците нема да бидат читливи од неавторизирани лица, како на пример користење на алатка за некрипција на дисковите на преносните компјутери (notebook), согласно член 40, IV. Високо Ниво, од Правилник за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци
- Тестирање на информацискиот систем - воведување на практика за редовно независно и професионално тестирање (како на пример Етичко хакирање) на механизмите и контролите за заштита на податоците и сајберзакан , согласно член 41, IV. Високо Ниво, од Правилник за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци

- Пренесување на личните податоци преку мрежа за електронски комуникации со користење на соодветни методи за енкрипција и заштита, согласно член 44, IV. Високо Ниво, од Правилник за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци

Член 20

За сите збирки Кинотека задолжително применува технички и организациски мерки кои се класифицирани на стандардно ниво.

Член 21

За збирките кои содржат: посебни категории на лични податоци, лични податоци кои се обработуваат заради заштита на безбедноста и интересите на државата, задолжителни се применуваат технички и организациски мерки кои се класифицирани на стандардно и високо ниво.

За збирките кои содржат матичен број на граѓанинот, задолжително применува технички и организациски мерки кои се класифицирани на стандардно и високо ниво.

Физичка безбедност

Член 22

Кинотека обезбедува соодветни услови на физичка заштита на компјутерските системи кои се користат за обработка, чување или дистрибуција на личните податоци.

Под физички сигурносни контроли во смисла на овој Правилник се подразбираат соодветни мерки за ограничување и контрола на физичкиот пристап и ракување со информациите и информативните средства, за заштита од надворешни влијанија и оштетувања како што се пожар, поплава, влага, електрично напојување, вандализам и саботажа.

Член 23

Кинотека дефинира физички сигурносен периметар односно сигурносни зони со цел физички да ги заштити информативните средства, согласно Член 26, Физичка безбедност од Правилник за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци.

Физичкиот пристап е соодветно контролиран и овозможен само на авторизирани лица – вработени и/или трети лица.

На вработените им се доделува пристап во просториите согласно нивните работни позиции и одговорностите поврзани со исполнување на нивните работни задачи.

Член 24

Систем салата претставува посебна категорија на сигурносна зона со највисок степен на рестрикција за влез и заштита.

Правила кои се однесуваат на системската соба, согласно Член 26, Физичка безбедност од Правилник за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци се како што следува:

- редовно да се прави тестирање на системите за надгледување и одржување на оптимални работни услови во просторијата;
- редовна проверка на клима уредите и опремата за заштита од пожари во систем салата;
- физичкиот пристап во систем салата е соодветно контролиран и овозможен само за авторизирани вработени. Надворешни – трети лица може да влезат во систем салата самоово присуство на соодветен овластен вработен.
- воспоставување на соодветен механизам за евиденција за влезот односно ревизорски логови за пристапот во сигурносните зони.
- Напојување со електрична енергија - хардверската и останата опрема е обезбедена од испад во редовното напојување или неконтролирани промени во напонот, преку соодветни механизми со кое ќе се обезбеди континуитет во работењето според спецификациите на производителот на опремата во случај на испад на редовното напојување со електрична енергија.

Мрежно поврзување и комуникација

Член 25

Кинотека применува соодветни контроли во компјутерската мрежа и електронските комуникации согласно Член 7, став (3) Управување со ризик од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци како што следува:

- инсталирана хардверска/софтверска заштитна мрежна бариера (анг. Firewall) и рутер помеѓу компјутерскиот систем и интернет или било која друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивањена системот;
- мрежните комуникации и сервиси се конфигурирани со соодветно ниво на рестрикции во контролата на пристапот;
- мрежните комуникации и сервиси се управувани од авторизиран персонал на начин да не биде загрозувана сигурноста и ефикасноста на процесите;
- далечинскиот пристап до мрежата и ресурсите се дозволува само за авторизирани корисници низ процес на автентикација, рестрикции во правата на пристап и соодветно ниво на сигурност при пренос на податоците;
- мрежниот капацитет и пропусната моќ на комуникациските линии се дизајнирани на начин кој ќе овозможи непречено и ефикасно изведување на процесите;
- воспоставен е соодветен систем на ревизорска трага за евидентирање, мониторинг и дојава на сигурносни настани поврзани со користењето на мрежните комуникации и сервиси.

Член 26

Безжичното поврзување е заштитено од пресретнување или неавторизирано менување.

Кинотека воспоставува правила за поставување на безжичното поврзување, согласно Член 7, став (3) Управување со ризик од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци како што следува:

- поставување на соодветна енкрипција на податоците кои се пренесуваат преку безжичната комуникација;
- поставување на соодветни механизми за автентикација на корисниците (како на пример Wi-Fi Protected Access II);
- забрана на пропаганција (broadcasting) на единствениот идентификатор на мрежното поврзување (*service set identifier – SSID*);
- практика за гаснење (затварање) на безжичната комуникација (access point) надвор од работно време и за време на викенди и празници;
- рестрикција на видот на сообраќајот и дозволеният проток на податоци (personal firewall).

Член 27

Кинотека согласно член 12, Обезбедување на опремата на која се врши обработката на личните податоци од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци, применува соодветни контроли за далечински пристап, како што следува:

- сите вработени што користат преносни компјутери, односно лаптопи, таблети или други паметни уреди се одговорни за заштита на деловните податоци кои може да ги има на истите, како и за самата физичка заштита, заштитата на неовластен пристап, сигурносни заштити и анти-вирусна заштита.
- мобилната и портабилната опрема која се користи и која има сензитивни и/или критични деловни информации не смее да се остави без надзор, и каде е можно физички да се заклучи.
- далечинскиот пристап до компјутерските системи и информациите е временски ограничен со автоматско прекинување на сесијата по истекување на даден временски период, секогаш кога тоа е можно и изводливо.

Интернет сервиси

Член 28

Електронската пошта (во понатамошниот текст: е-пошта) се користи за деловните потреби на Кинотека согласно интерните процедури како и законската регулатива.

Кинотека воспоставува правила за користење на е-пошта согласно член 30, Организационски мерки за безбедност на личните податоци (минимален стандард) од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци како што следува:

- само авторизирани лица од организационата единица за ИТ односно авторизирани од нив лица (надворешни добавувачи) се задолжени за конфигурација и поставување на системот за е-пошта;
- корисниците за е-пошта не смеат лажно да се преставуваат и да превземаат туѓ идентитет при комуникацијата;
- корисниците треба да ги користат прилозите во електронските пораки со максимална претпазливост и таквата содржина може да биде предмет на внатрешно филтрирање од страна на системот за електронска пошта.

На пример преносот на одреден тип на фајлови (exe, .bat, .pif, .mpeg, .mp3,.....) е забрането преку системот на е-пошта;

- потребно е да се воспостави и период на чување на електронска пошта за да се задоволат правни и деловни потреби и сите корисници на тој сервис мора да се придржуваат кон периодот на чување;
- не смее да се злоупотребува сервисот за е-пошта за вознемирување и пропагирање на неетички материјали и содржини;

Член 29

Интернет и интернет сервисите се користат за деловните потреби на Кинотека согласно интернетните процедури како и законската регулатива.

Кинотека воспоставува правила за користење на Интернет согласно, член 30, Организациски мерки за безбедност на личните податоци (минимален стандард) од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци како што следува:

- Интернет пристапот мора да биде воспоставен преку соодветни рестрикции за пристап, исполнувајќи го правилото на најмали привилегии;
- Интернет пристапот треба да биде обезбеден од надворешни малициозни упади преку постапување и конфигурирање на рестриктивен пристап кон интернет содржините преку огнени ѕидови (анг. firewall);
- Пристапот до Интернет и користењето на интернет сервисите (социјални мрежи, инстант комуникација - chat) не смее на никој начин да го загрози ефикасното и сигурно работење и изведување на деловните операции;
- Пристапот и користењето на Интернет сервисите е предмет на редовна контрола и мониторирање;
- Пребарувачите треба да се користат на сигурен начин со помош на вградените сигурносни алатки и функционалност;
- Вработените треба да бидат запознаени со правилата за сигурно користење на Интернет и Интернет сервисите.

Член 30

Кинотека применува 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, согласно, член 19, Обезбедување на веб-страницата на контролорот од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци преку следните мерки:

- имплементација на криптографски протокол (TLS / SSL) на сите веб страници на контролорот;
- 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
- при користење на колачиња, се обезбедува претходна согласност од интернет корисникот откако ќе го извести корисникот.

Обезбедување на серверите и персоналните компјутери на која се врши обработка на личните податоци

Член 31

Кинотека применува соодветни технички мерки со кои се обезбедува заштита на серверите и опремата, согласно Член 12, Обезбедување на опремата на која се врши обработка на личните податоци од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци како што следува:

- редовно ажуриран антивирусен софтвер и дефинирана политика за редовни ажурирања на софтверските програми;
- конфигурирани софтверски програми така што безбедносните ажурирања да се вршат автоматски;
- 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;
- ефективна и сигурна анти-спам заштита, која постојано се ажурира заради превентивна заштита од спамови;
- 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);
- автоматизирано одјавување на информацискиот систем после изминување на определен период од 15 минути на неактивност и за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;

Управување со корисници

Член 32

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

Кинотека има воспоставено 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.

Член 33

Пристапот до системите обезбедува минимум привилегии со цел се остварат работните задачи и обврски на вработените, ангажираните лица и/или други овластени лица согласно нивната работна позиција и деловните барања. (принцип “need to know”).

Правата на пристап се дизајнирани согласно правилото за сегрегација (поделба) на должности, секаде каде што тоа е можно.

Деловните барања за пристап и ниво на привилегија се дефинирани, документирани и соодветно авторизирани.

Кинотека има воспоставено процес за регистрација и контрола на правата на пристап до информативните системи. Процесот ги покрива сите фази од иницијалната регистрација на нови корисници, до конечното бришење на корисниците кои веќе немаат деловна потреба за пристап.

Администраторот на информацискиот систем е овластен од страна на Кинотека како контролор, ги доделува, менува или одзема привилегиите на авторизираниот пристап до личните податоци и информатичко комуникациската опрема само во согласност со законската и интерната регулатива.

Член 34

Кинотека има воспоставено соодветен процес за идентификација и автентикација на корисниците на информативниот систем, согласно Член 11, 1. Технички мерки Автентикација на овластените лица од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци.

Идентификација (анг. Identification) претставува процес на доделување на единствен идентификатор (корисничко име) за најава на системите.

Автентикација (анг. Authentication) е процес на потврда на идентитетот на корисникот (субјектот) и неговите права на пристап до системите.

Во зависност од критичноста на информативниот систем може да се употребат еден или повеќе начини за автентикација, како што се:

- ✓ со употреба на слог (низа) од знаци познати само на корисникот (како што е на пример употреба на лозинка);
- ✓ со употреба на уред кој единствено го поседува корисникот (пример електронска картичка);
- ✓ со употреба на биометриски карактеристики кои се единствени за корисникот (скенирање на око, отисок на прст).

Член 35

Кинотека ги применува правилата за регистрација на корисниците, односно постапка за доделување и одземање на права пристап кон информативните системи на сите нивоа (оперативен систем, бази на податоци и апликации) согласно Член 18, став (1) Обезбедување на серверите, од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци како што следува:

- користење на единствен идентификатор (корисничко име) со кој корисниците ќе бидат еднозначно поврзани;

- користењето на групни кориснички имиња или генерички (вградени) кориснички профили (пример `operator /administrator`) треба да се избегнува и да се применува само во исклучителни ситуации;
- креирање на права за пристап и ниво на привилегија согласно деловните потреби и во согласност со овластувањата;
- обезбедување на правила кои ќе спречат индивидуалниот пристап да не ја компромитира контролата за соодветна сегрегација на должности;
- воспоставување на соодветна ревизорска трага за пристапот и користењето на системите;
- постапки за промена односно укинување на пристапот при промена на работната позиција или напуштање.

Управување со лозинки

Член 36

Кинотека пропишува соодветни правила за избор и ракување со лозинките на корисничко и системско ниво за пристап до информативниот систем. Лозинките се најчестиот начин за обезбедувањена автентикација на корисниците, односно потврда и валидација на идентитетот на корисниците при пристап до информативните системи или сервиси.

Кинотека дефинира правила за ефикасен и сигурен систем за управување со лозинки согласно член 11, став (2), 1. Технички мерки Автентикација на овластените лица од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци како што следува:

- користење на индивидуални кориснички профили и лозинки за да се задржи одговорноста (accountability);
- менување на пред дефинираните лозинки (default passwords) за системите (сервери, мрежна опрема, бази на податоци, оперативни системи и слично);
- лозинката треба да биде составена од комбинација на најмалку осум алфанумерички карактери букви (мали и големи), симболи, броеви и интерпункциски знаци;
- 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.
- обезбеди механизам за заклучување на корисникот после одреден број на неуспешни најави, но не повеќе од пет последователни неуспешни обиди
- обезбеди механизам за чување на историја на користени лозинки на корисниците;
- заштита од повторна употреба на истите лозинки за даден временски период наназад;
- маскирање на лозинките на екран за време на нивно внесување;
- имплементација на сигурносни механизми за чување и пренос на лозинките (encrypted or hashed).
- иницијалните лозинки треба веднаш да се сменат при првата најава.

Член 37

Пристапот во креирањето на правилата за управување на лозинките е во согласност со критичноста на корисничките профили односно нивото на привилегија, како што се систем

администратори, сервисни, системски кориснички профили и слично, согласно член 18, Обезбедување на серверите од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци.

Член 38

Кинотека има посебни правила за креирање и употреба на лозинките за администраторите на информацискиот систем, согласно член 38, Високи мерки, Управување со лозинки од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци како што следува како што следува:

- лозинката треба да биде составена од комбинација на најмалку 12 алфанумерички карактери букви (мали и големи), симболи, броеви и интерпункциски знаци;
- лозинките задолжително автоматски се менуваат по изминат определен временски период врз основа на анализата на ризикот кој не може да биде подолг од еден месец.

Систем за мониторинг и контрола

Член 39

Кинотека има воспоставено ревизорската трага во критичните делови од информативниот систем и тоа на повеќе нивоа – оперативен систем, апликации, база на податоци и мрежна комуникација, периферни уреди (UPS), преку бележење (event recording), согласно Член 15, Обезбедување евиденција за секој пристап (logs) од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци на следниве параметри:

- корисничкото име ;
- датум и време на најавата и одјавата од системот;
- идентификатор на терминалот или доколку е можно локацијата;
- записи за успешни и одбиени обиди за најава;
- записи за успешни и одбиени податоци и други обиди за обиди за пристап.

Кинотека има воспоставено механизам за заштита на интегритетот на ревизорската трага односно менување во целиот нејзин животен век.

Член 40

Настаните од логовите, се предмет на континуиран мониторинг и контрола од соодветните ИТ лица – администратори на редовна основа.

Офицерот за заштита на личните податоци врши контрола на податоците од логовите од аспект на неавторизиран пристап на корисниците, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

План за континуитет и сигурносни копии

Член 41

Кинотека развива и одржува соодветен план за континуитет во работењето заедно со соодветните постапки и сценарија за сигурносни копии и реставрација со цел деловните процеси

и податоци (вклучително и личните податоци) да бидат зачувани и обновени во временски прифатлива рамка со цел да се минимизираат штетите направени при голем прекин односно катастрофа.

Мерките и активностите опфатени во рамките на Планот за континуитетот во работењето е базиран на процена на ризиците и нивното влијание врз деловните процеси, согласно член 22, Сигурносни копии и повторно враќање на зачуваните лични податоци (обезбедување континуитет) од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци.

Кинотека прави сигурносни копии на личните податоци на редовни временски интервали, со цел да го намали ефектот во случај на нивно непосакувано губење или оштетување.

Член 42

За максимална ефикасност, Планот за Континуитет и соодветните упатства за сигурносни копии (backup) и ИТ обнова е фокусиран на следниве принципи:

- заштита на животот и здравјето на вработените за време на катастрофа;
- заштита и поврат на податоци и информации по појавата на катастрофа, преку сигурносни копии на личните и други податоци на редовни временски интервали, со цел да го намали ефектот во случај на нивно непосакувано губење или оштетување.
- заштита на комуникациските линии и средствата и од информативниот систем.

Член 43

Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат серверите се физички и криптографски заштитени, заради оневозможување на каква било модификација и злоупотреба од неовластени лица., согласно член 22, став (5) Сигурносни копии и повторно враќање на зачуваните лични податоци (обезбедување континуитет) од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци.

Член 44

Планот за континуитет во работењето заедно со соодветните механизми за реконструкција периодично се проверуваат и тестираат, а најмалку еднаш годишно врз основа на однапред утврдени сценарија со цел да се обезбеди дека се во согласност со деловните активности и дека е актуелен.

Врвното раководство редовно е информирано за нивото на ризици односно ефикасноста на процесот за обезбедување на континуитет во работењето и податоците, преку редовните тестирања и соодветните извештаи.

ИТ Администраторите ја проверуваат функционалноста на сигурносните копии за вршење на реконструкција на личните податоци, на редовна основа.

Енкрипција

Член 45

Шифрирање (енкрипцијата) е техника за заштита на сензитивни или критични информации со цел да се обезбеди нивната доверливост, интегритет и неотповикливост во пристапот и користењето, согласно Член 17, Заштита на внатрешната мрежа од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци.

Потребното ниво на шифрирањето вклучувајќи го типот и квалитетот на алгоритмот за како и должината на клучевите за заштита кои ќе се користат, треба да е базирана на анализа и проценка на ризиците за критичноста на информациите.

Сензитивните и доверливи информации се чуваат и пренесуваат шифрирани секаде каде тоа е возможно. Забрането е испраќање на сензитивни информации и информации класифицирани со највисок степен на доверливост, како ЕМБР преку сервисите за електронска комуникација како што се електронска пошта, инстант комуникации и слично ако не се заштитени од неавторизирано читање и менување.

Овие техники и механизми мора да имаат можност за имплементација на соодветни механизми за дешифрирање на информациите од страна на авторизирани лица во точно определена постапка.

Обезбедување на преносливите медиуми

Член 46

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

Пренесувањето на медиумите од ставот надвор од работните простории се врши само со претходно овластување од страна на Контролорот.

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.

Член 47

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.

Член 48

Медиумите можат да се пренесуваат надвор од работните простории само ако личните податоци се енкриптирани 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 лицето овластено од него.

Член 49

Личните податоци (пример ЕМБР) можат да се пренесуваат преку електронска комуникациска мрежа, само ако се енкриптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи при преносот.

Справување со инциденти

Член 50

Според законската дефиниција, нарушувањето на безбедноста на личните податоци претставува настан кој доведува до случајно или незаконски уништување, губење, менување, неовластено откривање или пристап до личните податоци кои се пренесуваат, чуваат или на друг начин обработуваат.

Кинотека има воспоставено Правилник за начинот на известување за нарушување на безбедноста на личните податоци кои се обработуваат.

Член 51

Доколку некој настан се класифицира како нарушување на безбедноста на личните податоци кое претставува ризик за правата и слободите на субјектите на личните податоци, контролорот мора за тоа во рок од 72 часа да ја извести Агенцијата за заштита на личните податоци.

Управување со обработувачи

Член 52

Меѓусебните права и обврски на контролорот и надворешните компании кои согласно Законот за заштита на лични податоци се категоризирани како обработувачи, се уредени со соодветен договор.

Кинотека како Контролор пред да го склучи договорот е должен да побара од обработувачот (давател на услугата), да му ја презентира својата безбедоносна политика во однос информацискиот систем и информатичката инфраструктура на која ќе се врши обработката на личните податоци во име на Контролорот. Од особено значење е во договорот за outsourcing кој предвидува обработка на лични податоци да се наведат обврските и прецизна дистинкција помеѓу улогите на Контролор (т.е. клиент) и Обработувач (т.е. добавувач), кои произлегуваат од Законот за заштита на личните податоци.

Договорот треба да ја вклучува одредбата дека добавувачот ќе ги обработува личните податоци само според документираните упатства добиени од страна на клиентот и со примена на соодветни технички и организациски мерки.

Член 53

Како минимум Договорите со обработувачите мора да ги вклучат следниве елементи:

– обврските за обработувачот да преземе технички и организациски мерки за да обезбеди безбедност на обработката на личните податоци. При тоа обработувачот треба да ја земе предвид

чувствителната природа на личните податоци со примена на современи технолошки решенија и обврски кои треба да обезбедат заштита и доверливоста на обработката;

- условите за враќање на податоците и/или нивно уништување по истекот или раскинувањето на договорот;

- правилата за управување и известување на контролорот во случај на инциденти, односно во случај на нарушување на безбедноста на личните податоци;

- обврските за обработувачот да постапува единствено во согласност со упатствата добиени од страна на контролорот;

- сите вработени и вработените од обработувачот и нивните подизведувачите кои вршат обработка на личните податоци, пред нивното отпочнување со работа треба да потпишат Изјава за доверливост и тајност.

Кинотека како Контролор мора да биде информирана за сите подизведувачи кои се ангажирани при што истите треба да го имаат како минимум нивото на мерки кои ги обезбедува Обработувачот.

Чување на документација – правило на чисто биро

Член 54

Кинотека го промовира и 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, согласно Член 33, Правило „чисто биро“ од Правилникот за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци.

Член 55

Документацијата која се користи во Кинотека е сместена во простории и во засебни плакари (ормани) 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, Контролорот треба да примени други мерки за да се спречи секој неовластен пристап до документите.

Плакарите (орманите), картотеките или другата опрема за чување на документи кои содржат лични податоци 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.

Член 56

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

Рокови за чување на личните податоци

Член 57

Личните податоци се чуваат само за време додека е тоа потребно за постигнување на намената за која биле собрани, а потоа и обработени. При тоа се почитуваат роковите кои се предвидени согласно законите и интерните акти кои ја регулираат соодветната област, како и законот за архивско работење.

Тестирање (високо ниво)

Член 58

Кинотека врши тестирање на информацискиот систем пред неговото имплементирање или поизвршените промени со цел да се провери дали системот обезбедува безбедност на личните податоци согласно со прописите за заштита на личните податоци, согласно Член 41, IV. Високо Ниво, од Правилник за безбедност на обработката на личните податоци на Агенцијата за заштита на личните податоци. Обемот, фреквенцијата и предметот на тестирање на отпорноста на системите се определени во зависност од нивото на ризик од заканите од дигиталниот простор.

Периодична контрола

Член 59

Мерките за обезбедување на на тајност и заштита на личните податоци подлежат на 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.

Член 60

Внатрешната контрола се прави на годишно ниво или по потреба при значајни организациски и/или технички промени, барања од менаџментот и/или согласно законски и регулаторни барања.

Внатрешната контрола ја изведува Офицер за заштита на лични податоци за што подготвува соодветен извештај за степенот на усогласеност со Законот за заштита на личните податоци.

Член 61

Кинотека врши периодична оценка на постигнатите резултати од системот за вршење видео надзор на секои две години. Процесот на анализа и контрола на видео надзорот е опфатен со соодветниот Правилник за видео надзор.

Член 62

Офицерот за заштита на личните податоци најмалку еднаш месечно врши периодична контрола на неавторизираниот пристап до системите и работата на администраторот на

информацискиот систем и изработува извештај за извршената проверка и за констатираните неправилности.

Завршни одредби

Овој Правилник стапува на сила со денот на неговото усвојување.

Правилникот е предмет на редовни прегледи и ажурирања согласно промени во организациската поставеност, техничката инфраструктура или нови законски и /или регулаторни барања.

Бр. _____

Датум: _____

НУ Кинотека на Република Северна Македонија
Претседател на Управен Одбор

Томислав Османли