ПОЛИТИКА ЗА БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Систем за заштита на личните податоци

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, контролорот е должен да воспостави систем за заштита на личните податоци преку примена на соодветни технички и организациски мерки за да обезбеди ниво на безбедност соодветно на ризикот. Техничките и организациските мерки особено опфаќаат: - псевдонимизација и криптирање на личните податоци; - способност за обезбедување на континуирана доверливост, интегритет, достапност и отпорност на информацискиот систем за обработка; - способност за навремено, повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на физички или технички инцидент; и - процес на редовно тестирање, оценување и евалуација на ефективноста на техничките и организациските мерки со цел да се гарантира безбедноста на обработката. Контролорот врши оценка и ажурирање на техничките и организациските мерки при што секогаш ги применува оние мерки кои се соодветни на времето во кое се дизајнираат и имплементираат, а согласно најновите технолошки достигнувања (a state of the art technology). Процесот за управување со системот за заштита на личните податоци е дефиниран во Политиката за системот за заштита на личните податоци на контролорот кој треба да им одговара на природата, обемот и сложеноста на активностите коишто контролорот ги врши при обработката на личните податоци и ризиците на коишто е изложен. Контролорот е должен Политиката да ја ревидира и усогласува согласно промените во неговото работење.

Управување со ризик

Контролорот при утврдувањето и проценатa 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. Управувањето со ризикот ги опфаќа следните фази:

а) список (преглед) на сите процеси со кои се врши обработка на лични податоци; Списокот на процеси со кои се врши обработка на личните податоци преку целосно или делумно автоматизирана обработка на личните податоци или друга обработка на лични податоци, треба најмалку да ги опфати: - хардверот (на пример: сервери, лаптопи, хард дискови и други медиуми); - софтверот (на пример: оперативни системи и софтверски програми развиени за потребите на контролорот); - комуникациски канали (на пример: оптички кабли, интернет, безжична мрежна технологија – Wi-Fi); - документи во хартиена форма (на пример: печатени документи, фотокопии).

б) процена на ризиците за секој процес на обработка на лични податоци; Проценатa на ризиците треба најмалку да ги опфати: (а) утврдување на потенцијалните влијанија и ефекти врз правата и слободите на физичките лица на кои се однесува и тоа за следните потенцијални закани, односно настани: - неовластен пристап до личните податоци; - непосакувани промени на личните податоци; и - привремена или целосна недостапност до личните податоци. (б) идентификување на изворите на ризик кој што може да биде причина за секој непосакуван настан, а имајќи ги предвид внатрешните и надворешните човечки ресурси (на пример: администраторот на информацискиот систем, овластеното лице, надворешниот напаѓач, конкурент), како и другите внатрешни и надворешни извори (на пример: вода, опасни материјали, пожар, вирус). (в) идентификување на можните закани кои би можеле да се случат преку медиуми од кои зависат личните податоци (на пример: хардвер, софтвер, комуникациски канали, документи во хартиена форма, итн.), а кои може да бидат: - употребени на несоодветен начин (на пример: злоупотреба на овластувањата, грешка при ракување); - изменети (на пример: „заразен“ софтвер или хардвер – keylogger, инсталирање на злонамерен софтвер, итн); - изгубени (на пример: кражба на лаптоп или губење на мемориски уред – УСБ); - набљудувани (на пример: гео-локација на опремата); - оштетени (на пример: вандализам, деградација заради природно абење); - преоптоварени (на пример: медиумот за складирање е целосно пополнет, denial of service attack и сл.). (г) Утврдување на постојни или планирани мерки што овозможуваат решавање на секој ризик (на пример: контрола на пристап, сигурносни копии, информациска ревизорска трага, безбедност на просториите, криптирање или анонимизација). (д) Оценување на сериозноста и веројатноста на ризиците, во однос на претходните елементи предвидени во овој став (на пример: скала што може да се користи за проценка: занемарлива, умерена, значајна и максимална) в) спроведување и проверка на планираните мерки; Контролорот задолжително врши спроведување и проверка на планираните мерки а со цел да се обезбеди дека тие се применуваат и тековно се тестираат. и г) спроведување на периодични безбедносни проверки. Контролорот задолжително спроведува периодични безбедносни проверки за што се подготвува акционен план, чија имплементација се следи од страна на раководството на контролорот.

Нивоа на мерки за безбедност на обработката на личните податоци

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 од се класифицираат во две нивоа: - стандардно; и - високо. Контролорот кој обработува лични податоци за помалку од 10 вработени како единствена збирка на лични податоци, нема обврска да примени технички и организациски мерки освен ако постои веројатност дека обработката која што ја врши

претставува ризик за правата и слободите на субјектите на личните податоци, ако обработката не е повремена или обработката вклучува посебни категории на лични податоци или лични податоци поврзани со казнени осуди и казнени дела.

Примена на нивоа на мерки за безбедност на обработката на личните податоци

Контролорот е одговорен за усогласеноста во однос на нивото на мерки за безбедност на обработката на личните податоци 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. Контролорот ја демонстрира примената на мерките вклучувајќи ги причините и основите за изборот на примената на стандардното, односно високото ниво.

СТАНДАРДНО НИВО

Документација за технички и организациски мерки

Контролорот 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, контролорот донесува подетални политики и процедури во кои се опишани техничките и организациски мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем и информатичка инфраструктура.
Документираните процеси се однесуваат на:
- идентификацијата, оценката и класификацијата на ризикот на процесите со кои се врши обработка на личните податоци (анализа на ризик);
- општ опис на техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци соодветно на ризикот;
- активности за обука и подигнување на свеста на раководството и вработените за приватноста и безбедносните ризици во контролорот;
- дизајнирање, развивање и одржување на софтверските програми за обработка на личните податоци, а особено од аспект на техничка и интегрирана заштита на личните податоци (Data protection by design and by default);
- начинот на обезбедување на автентикација на овластените лица во информацискиот систем;
- начинот на обезбедување на контрола на пристап до информацискиот систем;
- начинот на обезбедување евиденција за секој пристап до информацискиот систем,
- начинот на управување со инциденти (инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци);
- начинот на обезбедување на опремата на контролорот на која се врши обработка на личните податоци;
- начинот на обезбедување на преносливите медиуми;
- начинот на заштита на внатрешната мрежа на контролорот;
- начинот на обезбедување на серверите и веб-страницата на контролорот;
- начинот на евидентирање и чување на документацијата за софтверските програми за

обработка на личните податоци;
- начинот на обработка на личните податоци кои се псевдонимизирани;
- начинот на обработка на личните податоци кои се криптирани;
- обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема;
- начинот и процесите за пријавување, реакција и санирање на инциденти;
- начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;
- начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите;
- физичка безбедност;
- начинот на ангажирање и контрола на надворешни субјекти (обработувачи);
- динамика и начин на вршење на периодични контроли, како и процесите за вршење на внатрешна контрола; и
- други мерки кои контролорот ги применува врз основа на анализата на ризикот.

Документацијата, контролорот ја менува и дополнува кога ќе се направат промени во информацискиот систем и информатичката инфраструктура, а најмалку еднаш годишно врши нејзино оценување, евалуација и ажурирање.

1. Технички мерки

Автентикација на овластените лица

Контролорот обезбедува најавата во информацискиот систем да се врши преку единствен идентификатор кој се поврзува само со едно овластено лице.

Единствениот идентификатор контролорот 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;
- нешто што само овластеното лице го поседува (на пример: паметна картичка – smart card);
- нешто што овластеното лице е, или го прави (на пример: дигитален потпис); и
- други начини на автентикација кои според најновите технолошки достигнувања, а во контекст на извршената анализа на ризикот обезбедуваат единствен идентификатор кој се поврзува само со едно овластено лице.

Автентикацијата на овластените лица, контролорот ја врши најмалку преку еден од претходно наведените. Во зависност од анализата на ризикот, за одредени овластени лица или за сите, може да се примени и комбинација од два или повеќе фактори на автентикација (на пример: единствено корисничко име и лозинка во комбинација со употреба на паметна картичка).

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

Кога проверката се врши врз основа на корисничко име и лозинка, контролорот 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

Контролорот 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 информацискиот систем после изминување на определен период на неактивност (не подолго од 15 минути). За повторно активирање на системот, контролорот треба да обезбеди дека овластените лица пристапуваат со примена на автентикацијата.
- во случај на одреден број на неуспешни обиди за најавување на информацискиот систем, кои се во спротивност со политиките за автентикација на контролорот, треба да се обезбеди автоматизирано отфрлање од информацискиот систем. Бројот на неуспешни обиди контролорот 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 контролорот;
- 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 контролорот за кои редовно се прави сигурносна копија, а во случај кога податоците се зачувуваат локално, задолжително со мерки за синхронизација или со резервни дополнителни мерки за заштита врз основа на анализа на ризикот;
- 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 информацискиот 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 информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.
Покрај овие мерки а врз основа на спроведената анализа на ризик, доколку се утврди за потребно, контролорот 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 информацискиот систем на контролорот, со цел откривање дали се загрозени и други елементи;
- безбедносен надзор на софтверот и хардверот што се користи во системот на контролорот, 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 контролорот.

Сегрегација на должности и одговорности

Контролорот ги утврдува овластените лица кои треба да имаат пристап до информацискиот систем при што обезбедува јасна поделба на должностите и одговорностите според правилото „потребно е да знае“, односно дека овластеното лице ќе има пристап само до оние лични податоци за кои има неопходна потреба заради извршување на своите должности.
Контролорот обезбедува повлекување на правата на пристап веднаш по престанокот на овластувањата за пристап.
Контролорот врши проверка и ажурирање на привилегиите за пристап до информацискиот систем на овластените лица. Проверката се врши за периоди кои се определуваат врз основа на анализата на ризикот, а најмалку квартално.

Контрола на пристап до информацискиот систем

Овластените лица задолжително имаат авторизиран пристап само до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работни задачи.
Контролорот воспоставува механизми за да се оневозможи пристап на овластенит лица до личните податоци и информатичко комуникациската опрема со права различни од тие за кои се авторизирани.
Администраторот на информацискиот систем кој е овластен од контролорот, ги доделува, менува или одзема привилегиите на авторизираниот пристап до личните податоци и информатичко комуникациската опрема само во согласност со критериумите кои се утврдени од страна на контролорот.

Обезбедување евиденција за секој пристап (logs)

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

Евиденцијата треба да ги содржи особено следните податоци: име и презиме на овластеното лице, работната станица од каде се пристапува до информацискиот систем, датум и време на пристапување, лични податоци кон кои е пристапено, видот на пристапот со операциите кои се преземени при обработка на податоците, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.

Во евиденцијата 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.

Операциите кои овозможуваат евидентирање на податоците треба да бидат контролирани од страна на офицерот за заштита на личните податоци и/или од друго овластено лице од контролорот 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, контролорот може да користи и алатки кои податоците ги генерираат во едноставна и лесно разбирлива форма за читање. Евиденцијата се чува најмалку пет години.

Офицерот за заштита на личните податоци врши контрола на податоците од најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

Контролорот ги известува овластените лица за воспоставениот систем за евиденција за пристап до информацискиот систем.

Контролорот обезбедува заштита на системот за евиденција за пристап до информацискиот систем, од било каков неовластен пристап, особено на лицата чија активност се евидентира на системот за евиденција.

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

Контролорот 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.

Контролорот не смее да ги користи информациите од евиденцијата за пристап до информацискиот систем за цел различна од таа дека информацискиот систем се користи соодветно (на пример: употреба на записите за мерење на часовите на вработениот претставува злоупотреба на информацискиот систем).

Обезбедување на преносливите медиуми

Контролорот согласно анализата на ризикот од нарушување на безбедноста на личните податоци во случај на кражба или друг начин на загуба на преносливите медиуми (мобилна опрема) на кои се врши обработка на личните податоци применува соодветни технички мерки.
Техничките мерките го опфаќаат најмалку следното:
- подигање на свеста на овластените лица за специфичните ризици поврзани со користење на преносливи медиуми (на пример: кражба на опремата) и утврдените процедури за намалување на овие ризици;
- спроведување на мерки за правење на сигурносна резервна копија или синхронизација на мобилните работни станици, со цел да заштитат од губење на зачуваните податоци;
- мерки за криптирање за заштита на мобилни работни станици и медиуми за мобилно складирање (лаптоп, УСБ, надворешни хард-дискови, ЦД-РОМ, ДВД, итн.). На пример: повеќето лаптопи вклучуваат функционалност што овозможува да се криптира нивниот хард диск поради што секогаш кога е можно, е препорачливо да се користи оваа опција); и
- употреба на услуги во облак (cloud services) за правење на сигурносни копии само по претходна анализа на нивните услови и безбедносни гаранции.
Покрај овие мерки, врз основа на спроведената анализа на ризик, доколку се утврди за потребно, контролорот може да ги примени и следните мерки:
- поставување на филтер за приватност на екраните на мобилните работни станици што се користат на јавни места, или употреба на мобилни работни станици со интегриран филтер за приватност;
- ограничување на обемот на податоци кои може да се зачуваат на мобилните работни станици на она што е строго неопходно со дополнителна заштита и ограничување за време на патувања, особено во странство;
- спроведување на дополнителни мерки за заштита од кражба (на пример кабел за безбедност, видливо обележување на опремата итн) и мерки што ги намалуваат негативните ефекти (на пример автоматско заклучување, криптирање); и
- кога мобилните уреди се користат за собирање податоци во движење (на пример: лични асистенти, паметни телефони, лаптопи, итн.), шифрирање на податоците на самиот уред. Исто така, заклучување на уредот по неколку минути неактивност и прочистување на податоците собрани веднаш штом се пренесат во информацискиот систем на контролорот.

Заштита на внатрешната мрежа

Контролорот 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 sиd, 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).

Контролорот врз основа на анализата на ризикот, покрај претходните мерки, може да примени и други мерки со кои ќе ја зајакне заштитата на својата и внатрешна мрежа.

Обезбедување на серверите

Контролорот 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 контролорот 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 информацискиот систем (вообичаени операции за стандардни корисници);
- примена на посебна политика за креирање и употреба на лозинките за администраторите на информацискиот 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, контролорот 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 контролорот

Контролорот 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 контролорот (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, контролорот обезбедува претходна согласност од интернет корисникот откако ќе го извести корисникот, а пред да се депонира колачето;
Контролорот 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 информацискиот систем и на овластените лица

Контролорот врз основа на спроведената анализа на ризик, ги определува обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема, применувајќи ги најмалку мерките кои се предвидени со овој правилник.
Контролорот задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.
Во извештајот се наведуваат констатираните неправилности (доколку ги има) и предложените мерки за отстранување на тие неправилности.

Контролорот задолжително ги информира администраторот и овластените лица за документацијата за технички и организациски мерки која се однесува на извршувањето на нивните обврски и одговорности.

Превенирање, реакција и санирање на инциденти

Контролорот врз основа на анализата на ризик утврдува план за управување со континуитет на својот информациски систем, вклучувајќи и список на овластените лица кои се одговорни за превенирање, како и за навремено повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на настанат физички или технички инцидент.

Согласно претходно наведеното, контролорот го определува начинот на управување со инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци.

Управувањето со инциденти, опфаќа пријавување, реакција и санирање на инцидентите, при што контролорот го определува начинот на евидентирање на секој инцидент, времето кога се појавил, овластеното лице кој го пријавило, на кого е пријавен и мерките кои се преземени за негово санирање.

Контролорот ги определува постапките кои се применуваат за повторно враќање на личните податоци и начинот на евидентирање на овластените лица на овој член, кои ги извршиле операциите за повторно враќање на личните податоци, категориите на личните податоци кои се вратени или кои биле рачно внесени при враќањето.

Контролорот обезбедува дека овластените лица, обработувачите и подобработувачите знаат кого да го известат и предупредат во случај на настанат инцидент.

Превенирањето на инцидентите ги опфаќа сите мерки и контроли утврдени со овој правилник, а врз основа на спроведената анализа на ризик (на пример: користење на непрекинато напојување за да се заштити опремата што се користи за обработка на личните податоци, едновремена употреба на повеќе уреди во низа за зачувување на личните податоци /RAID технологија/, редовно тестирање на функционалноста на уредите и слично).

Сигурносни копии и повторно враќање на зачуваните лични податоци

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

Сигурносните копии треба да се прават и тестираат редовно, за што контролорот усвојува План за обезбедување континуитет (business continuity plan) кој ги предвидува сите можни инциденти (на пример: хардверски инцидент).

Контролорот врз основа на анализата на ризикот, обемот и временската динамика на промена на податоците, прави сигурносни копии во интервали кои го минимизираат ризикот врз ефектот на податоците за кои при инцидент би настапило нивно непосакувано губење или оштетување. Притоа, контролорот прави фрагментирана (incremental back-up), односно поединечна копија на дневна основа во однос на сите настанати промени во текот на денот, а целосна сигурносна копија (full back-up) во редовни временски интервали по негова оценка, а најмалку еднаш месечно, на начин кој

ќе гарантира повторно воспоставување на достапноста до личните податоци во случај на настанат физички или технички инцидент.
Контролорот задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личните податоци.
Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат серверите и треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.
Контролорот во однос на сигурносните копии го применува истото безбедносно ниво на технички и организациски мерки како и за податоците кои се зачувани на оперативните сервери на кои врши обработка на личните податоци (на пример: со криптирање на сигурносните копии, со чување на безбедно место на сигурносната копија за кое се применети мерки и контроли кои го минимизираат ризикот од поплава, пожар, кражба и слично, или во случај на договорно регулирање и аутсорсирање на услугата, соодветна заштита која треба да ја примени и обработувачот).

Начин на архивирање и чувањена податоците

Контролорот, во однос на личните податоци за кои сè уште не истекол рокот за нивно чување согласно закон, а за кои престанала потребата од нивна непосредна и секојдневна обработка, врши архивирање на безбеден начин, особено ако архивираните податоци се чувствителни податоци (посебни категории на лични податоци), или податоци што можат да имаат сериозно влијание врз субјектите на личните податоци, доколку бидат компромитирани.
Согласно претходно наведеното, контролорот определува постапка за управување со архивскиот материјал во однос на тоа кои податоци треба да се архивираат, како и каде се чуваат и кој, како и под кои услови има пристап до нив.
Контролорот задолжително донесува соодветен документ „Список (преглед) со рокови на чување на личните податоци“ во кој ќе бидат содржани информации за моментот на активирање на периодот (рокот) за чување на личните податоци, идентификуваните периоди (рокови) за чување на личните податоци, причините за чување на личните податоци, законскиот основ за чување на личните податоци и сопственикот на податоците.
Контролорот е должен документот да го ревидира и усогласува годишно согласно промените во работењето на контролорот и законските услови за чување на личните податоци.

Управување со преносливи медиуми

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 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.

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.
Во тие случаи контролорот 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.

Криптирање на личните податоци

Кога контролорот врз основа на анализата на ризикот, а земајќи ги предвид природата, обемот, контекстот и целите на обработката на личните податоци, врши криптирање на личните податоци, секогаш применува најсовремени технички решенија за криптирање со кои го обезбедува интегритетот, доверливоста и автентичноста на личните податоци.
Контролорот применува единствено признати и безбедни алгоритми за криптирање (како на пример: SHA-256, SHA-512 или SHA-341 како хаш функција, HMAC користејќи SHA-256, bcrypt, scrypt или PBKDF2 за чување лозинки, AES или AES-CBC за симетрично криптирање, RSA-OAEP v2.1 за
асиметрично криптирање...), а воедно обезбедува заштита на тајните клучеви за криптирање со ограничувачки права за пристап и посебно креирана безбедна лозинка за пристап.
Контролорот донесува внатрешна процедура во која задолжително се пропишува начинот на управување со тајните клучеви и сертификати, земајќи го предвид и управувањето со ризикот на заборавени лозинки.

Физичка безбедност

Контролорот задолжително применува зајакнато ниво на безбедност во однос на просториите во кои се сместени и се чуваат серверите и мрежната опрема преку кои се врши обработка на личните податоци со примена на соодветни мерки кои обезбедуваат дека само лица посебно овластени од контролорот имаат пристап, како и мерки со кои се намалува ризикот од потенцијални закани и тоа:
- инсталирање на алармни системи против упад и нивна периодична проверка;
- примена на мерки и контроли за превенција од кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење;
- обезбедување безбедност на клучевите и шифрите за аларми кои овозможуваат пристап до просториите;
- обезбедување на одделни области во објектот каде се чуваат серверите според анализата на ризик (на пример: употреба на посебна контрола за пристап за сервер салата);
- ажуриран список на лица или категории на лица кои се овластени да влезат во просториите каде се чува опрема на која се врши обработка на личните податоци;

- воспоставување на правила и методи за контрола на пристапот на посетителите и тоа минимум со придружба од едно лице во контролорот со посетителите надвор од областите за прием на странки;
- посебна физичка заштита на ИТ-опремата преку специфични методи (систем за спречување на пожар, поплави, електрична енергија, климатизација, итн.);
- одржување на просториите за серверите (климатизација, UPS, итн.).
- водење на евиденција за пристап до просториите каде што се чуваат серверите кои содржат лични податоци;
- обезбедување дека само овластените лица можат да пристапат до просториите со ограничен пристап (на пример: во внатрешноста на контролираните простории за пристап, сите лица да носат видлива идентификација (картичка), како и преиспитување и редовно ажурирајте на дозволите за пристап до заштитените области).

По исклучок, серверите на кои се инсталирани софтверски програми за обработка на личните податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на контролорот. Во овој случај, меѓусебните права и обврски на контролорот 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 мерки за безбедност на личните податоци согласно прописите за заштита на личните податоци.

Контрола на информацискиот систем и информатичката инфраструктура

Во документацијата за технички и организациски мерки, 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.

Информацискиот систем и информатичката инфраструктура на контролорот 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.

Управување со обработувачи

Контролорот е должен да воспостави процес на управување при користење на услуги за обработка на личните податоци од страна на обработувачи, а со цел да се воспостават соодветни процедури за одлучување при изборот на обработувачот, управување со обработката на личните податоци, како и исполнување на договорените обврски и одговорности од страна на обработувачот.

Контролорот е должен да применува процедура за одлучување за избор на обработувач со која задолжително ќе предвиди:

1. Анализа на потенцијалните обработувачи во однос на нивните технички и организациски мерки за обезбедување на гаранција дека обработката на личните податоци ќе се одвива во согласност со барањата предвидени во прописите за заштита

на личните податоци, како и за обезбедување на заштита на правата на субјектите на лични податоци;и
2. Анализа на ризиците врз работењето на контролорот што можат да произлезат при обработката на личните податоци од страна на обработувачите.

Ангажирање на обработувачи

Во случај кога контролорот ќе одлучи да пренесе работи од неговиот делокруг на работа поврзани со обработка на лични податоци на обработувачот, должен е да обезбеди дека личните податоци се обработуваат под негов надзор над безбедноста на личните податоци, при што личните податоци мора да бидат обработувани со безбедносни гаранции. Контролорот може да пренесе работи само на обработувач кој може да обезбеди доволно гаранции, особено во однос на потребното знаење од областа на заштитата на личните податоци, сигурноста и ресурсите.
Меѓусебните права и обврски на контролорот и обработувачот мора да бидат уредени со договор при што контролорот пред да го склучи договорот е должен да побара од обработувачот (давател на услугата), да му ја презентира својата безбедносна политика во однос информацискиот систем и информатичкта инфраструктура на која ќе се врши обработката на личните податоци во име на контролорот.
Безбедносната политика треба да содржи податоци со кои ќе се гарантита безбедноста на личните податоци, и тоа:
- дали и како се врши криптирање на податоците според нивната чувствителност;
- постоење на процедури кои гарантираат дека никој нема да има неовластен пристап до податоците;
- дали и како се врши криптирање на преносот на податоци;
- гаранции во однос на следливост (логови, информациска ревизорска трага...);
- управување со правата на пристап;
- автентикација; и
- други мерки за безбедност на обработката на личните податоци.
Договорот треба да содржи одредби особено за:
- предметот, должината и целта на обработката на личните податоци;
- обврските за обработувачот да преземе технички и организациски мерки за да обезбеди безбедност на обработката на личните податоци;
- обврските во однос на доверливоста на доверените лични податоци;
- минималните стандарди за автентикација на овластените лица;
- 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; и
- другите обврски и одговорности согласно со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

2. Организациски мерки
Организациски мерки за безбедност на личните податоци

Контролорот 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:
1. Ограничен пристап со 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 каде што 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.
Вработеното лице кое ги врши работите за човечки ресурси кај контролорот, го известува администраторот на информацискиот систем за вработувањето или ангажирањето на секое овластено лице со право на пристап до информацискиот систем, за да му биде доделено корисничко име и лозинка, како и за престанок на вработувањето или ангажирањето за да му бидат избришани корисничкото име и лозинката, односно заклучени за натамошен пристап.
Известувањето се врши 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 информацискиот систем.

Информирање и едуцирање за заштитата на личните податоци

Лицата кои се вработуваат или се ангажираат кај контролорот, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.
За лицата кои се ангажираат за извршување на работа кај контролорот во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.
Контролорот 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 кај контролорот, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.
Изјавата 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 контролорот, освен ако со закон поинаку не е уредено и ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита.
Изјавата задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат кај контролорот.

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

Пристап до документите

Пристапот до документите треба биде ограничен само за овластени лица на контролорот. 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“

Контролорот 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

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, контролорот треба да примени други мерки кои што ќе го спречат секој неовластен пристап до документите.
Ако документите не се чуваат заштитени, тогаш контролорот треба да ги примени сите мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Уништување на документи

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

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, контролорот треба да примени други мерки за да се спречи секој неовластен пристап до документите.

ВИСОКО НИВО
Технички мерки
Дополнителни мерки

Контролорот 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.

Управување со лозинки

Контролорот треба да користи алатки за управување со лозинки со кои обезбедува дека различните лозинки за секоја услуга, или софтверска програма соодветно се чуваат, при што за пристап до сите лозинки обезбедува главна лозинка (master password), која треба да биде зајакнато комплексна, односно да биде составена од комбинација на најмалку 12 алфанумерички карактери (букви /мали и големи/), симболи, броеви и специјални интерпукциски знаци) и да се менува во период не подолг од 30 дена.

Контролорот во согласност со анализата на ризикот, за одредени овластени лица (на пример за администраторот на информацискиот систем или лицата кои креираат и користат главна лозинка (master password), може да изврши дисперзија на ризикот преку управување со лозинката со дополнителен фактор согласно правилото n-2 (на пример: информацијата за лозинката да биде поделена на две или повеќе лица кои заеднички ќе се најавуваат на начин што секој ќе знае само дел од информацијата која ја сочинува лозинката, или едно овластено лице ја знае лозинка, а друго ја поседува и употребува паметна картичка – smart card).

Сертификација за заштита на личнит податоци

Контролорот, покрај внатрешната контрола, а на доброволна основа, може да изврши и проверка на процесите и интерните документи за заштита на личните податоци заради сертификација на процесите преку кои се обработуваат личните податоци, со цел да демонстрира усогласеност со прописите за заштита на личните податоци при операциите на обработка. Сертификацијата се врши од Агенцијата или од сертификациони тела согласно прописите за заштита на личните податоци.

Управување со преносливи медиуми

Контролорот е должен да воспостави 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. Овие одредби се применуваат и за евидентирање на медиумите кои се испраќаат од страна на контролорот.

За пренесените медиуми надвор од работните простории на контролорот, треба да бидат преземени неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.

Тестирање на информацискиот систем

Контролорот задолжително врши тестирање на информацискиот 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 се врши преку обработка на документи кои содржат имагинарни лични податоци.

Сертификациони постапки

Контролорот може да применува и други технички мерки за тајноста и заштита на обработката на личните податоци, преку примена на сертификациони постапки согласно прописите што ја уредуваат употребата на електронски документи, електронска идентификација и доверливи услуги.

Пренесување на медиуми

Медиумите можат да се пренесуваат надвор од работните простории само 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.

Пренесување на личните податоци преку мрежа за електронски комуникации

Личните податоци можат да се пренесуваат преку мрежата за електронски комуникации само ако се криптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи при преносот.

Организациски мерки
Копирање и умножување на документите

Копирањето или умножувањето на документите може да се врши единствено од страна на овластени лица определени со процедура од страна на контролорот 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

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

Национално здружение за помош и поддршка на лица
со мултипла склероза - НАЦИОНАЛНО ЗДРУЖЕНИЕ ЗА МС

20.09.2021година

Претседател,

Ана Карајанова - Димитрушева

СПРОВЕДУВАЊЕ НА ПОЛИТИКАТА ЗА БЕЗБЕДНОСТ НА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ
(опис на технички и организациски мерки)

1. Сиситем за заштита на лични податоци
   – управување со ризик
   Личните податоци со кои располага Националното здружение за помош и подршка на лица со мултипла склероза - НАЦИОНАЛНО ЗДРУЖЕНИЕ ЗА МС Скопје се чуваат на посебен уред за зачувување во дигитална форма (виртуелен drive) со уникатна лозинка, достапна само на лицата кои имаат овластување за обработка на лични податоци, а дел од податоците кои се однесуваат здравствената состојба односно работниот и пензискиот статус се чуваат во хартиена форма во сеф/ормар со клуч.

-Процена на ризици – неовластен пристап, непосакувани промени и привремена или целосна недостапност на податоците

-извор на ризик – човечки ресурси – конкурент, надворешен напаѓач, овластено лице администратор или внатрешни и надворешни извори- вода, пожар и тн.

-можни закани на документи во хартиена форма – употреба на несоодветен начин(злоупотреба на овластување, грешка при ракување), губење, набљудување, оштетување и сл.

-утврдување на постојани или планирани мерки за решавање на секој ризик – Овластените лица за пристап до податоците имаат клуч од сеф/плакар каде се чуваат личните податоци .

СТАНДАРДНО НИВО НА МЕРКИ ЗА БЕЗБЕДНОСТ НА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

Документирани процеси за незбедност на обработка на личните податоци:

1. Анализа на ризик

2. Опис на технички и организациски мерки за обезбедување на тајност и заштита на обработка на лични податоци соодветно на ризикот
3. Активности за обука и подигнување на свеста на раководството и вработените за приватноста и безбедноста на ризици – офицерот за заштита на лични податоци редовно ја посетува страницата на Агенцијата за заштита на лични податоци, ги разгледува и спроведува сите новости и измени во Законите и правилниците за заштита на лични податоци за што следи редовни обуки од Агенцијата а за што редовно усно или писмено ги известува раководството и овластените лица за пристап до лични податоци за примена на истите.
4. начин на обезбедување на автентикација на овластените лица - Секое лице кое има пристап до лични податоци потпишува Изјава за тајност и заштита на обработката на лични податоци.
5. начинот на управување со инциденти (инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци)-брза рекација со воспоставување на конкретни системи.
6. Секој инцидент се пријавува кај раководните структури и офицерот за заштита на лични податоци.
7. Физичките документи се уништуваат со шредер – доколку нема со ситно кинење-сецкање на документите.
8. Сите документи кои содржат лични податоци се чуваат во сеф-ормар со клуч.
9. Спроведувањето на мерките е контролирано од раководството кое врши редовна внатрешна контрола еднаш годишно или по потреба.

20.09.2021 година

Претседател,

Ана Карајанова - Димитрушева