Врз основа на член 66 став (6) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија" бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе	Në bazë të nenit 66 paragrafi (6) i Ligjit për Mbrojtjen e të Dhënave Personale (Gazeta Zyrtare e Republikës së Maqedonisë së Veriut nr. 42/20), Drejtori i Agjencisë për Mbrojtjen e të Dhënave Personale solli
ПРАВИЛНИК	**RREGULLORE**
ЗА БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ	**PËR SIGURINË E PËRPUNIMIT TË TË DHËNAVE PERSONALE**
I. ОПШТИ ОДРЕДБИ	**I. DISPOZITAT E PËRGJITHSHME**
Предмет на уредување	**Lënda e rregullimit**
Член 1	**Neni 1**
Со овој правилник се пропишуваат упатства за постапување на контролорите при применувањето на техничките и организациските мерки за обезбедување на безбедност на обработката на личните податоци.	Kjo Rregullore përcakton udhëzime për veprimin e kontrollorëve gjatë zbatimit të masave teknike dhe organizative për të siguruar përpunimin e të dhënave personale.
Поимник	**Fjalor**
Член 2	**Neni 2**
Одделни изрази употребени во овој правилник го имаат следново значење:	Disa shprehje të përdorura në këtë Rregullore kanë këtë kuptim:
1. **Доверливост** е пристап до личните податоци единствено од лица кои имаат овластување за нивна обработка од страна на контролорот;	1. **Besueshmëria** është qasja në të dhënat personale vetëm nga persona që kanë autorizim për t'i përpunuar ato nga kontrolluesi;
2. **Интегритет** е заштита на точноста на личните податоци, при што се гарантира дека личните податоци се точни, целосни и ажурирани;	2. **Integriteti** është mbrojtja e saktësisë së të dhënave personale, me ç'rast garantohet se të dhënat personale janë të sakta, të plota dhe të përditësuara;
3. **Достапност** е непречен пристап и континуирана расположливост (business	3. **Qasshmëria** është qasja e papenguar dhe disponueshmëria e vazhdueshme (business

continuity) на информацискиот систем на кој се врши обработка на личните податоци од страна на овластените лица;	continuity) e sistemit të informacionit mbi të cilin kryhet përpunimi i të dhënave personale nga personat e autorizuar;
4. **Автентикација** е постапка која што овозможува потврдување на идентитетот на овластеното лице кое се најавува и пристапува на информацискиот систем на кој се врши обработка на личните податоци	4. **Autentifikimi** është procedurë që mundëson vërtetimin e identitetit të personit të autorizuar i cili regjistrohet dhe hyn në sistemin e informacionit në të cilin përpunohen të dhënat personale;
5. **Неотповикливост** е обезбедување на потврда на автентичноста на идентитетот на овластеното лице кое се најавува на информацискиот систем при што овластеното лице не може да ја негира преземената активност или дејствие	5. **Parevokueshmëria** është sigurimi i konfirmimit të autenticitetit të identitetit të personit të autorizuar i cili është futur në sistemin e informacionit, ku personi i autorizuar nuk mund të mohojë veprimtarinë ose veprimin e ndërmarrë;
6. **Безбедносен ризик**, е веројатност на случување на настан кој може да резултира со компромитирање, особено случајно или незаконско уништување, губење, менување, неовластено откривање на личните податоци, или неовластен пристап до пренесените, зачуваните или на друг начин обработени лични податоци (во натамошниот текст: ризик);	6. **Rreziku i sigurisë** paraqet mundësinë që një ngjarje të rezultojë me cenim të sigurisë, veçanërisht shkatërrim aksidental ose të paligjshëm, humbje, ndryshim, zbulim të paautorizuar të të dhënave personale, ose qasje të paautorizuar në të dhënat personale të transmetuara, të ruajtura ose në mënyrë tjetër të përpunuara (në tekstin e mëtejshëm: rreziku);
7. **Управување со ризик** е идентификација, оценка и негова класификација, која опфаќа координирана примена на ресурси на контролорот за минимизирање, набљудување и контрола на веројатноста и сериозноста која што може да произлезе при обработката на личните податоци, а која може да предизвика материјална или нематеријална штета врз процесите со кои се врши обработка на личните податоци;	7. **Menaxhimi me rrezikun** është identifikimi, vlerësimi dhe klasifikimi i tij, që përfshin zbatimin e koordinuar të resurseve të kontrolluesit për të minimizuar, vëzhguar dhe kontrolluar probabilitetin dhe seriozitetin që mund të paraqitet nga përpunimi i të dhënave personale, e që mund të shkaktojë dëm material ose jomaterial ndaj proceseve me të cilat bëhet përpunimi i të dhënave personale;
8. **Систем за заштита на личните податоци** е збир од документирани политики, кодекси на практика, насоки, процедури и работни инструкции донесени од страна на контролорот, а кои се во функција на	8. **Sistemi për mbrojtjen e të dhënave personale** është tërësi e politikave të dokumentuara, kodeve të praktikës, udhëzimeve, procedurave dhe udhëzimeve të punës të miratuara nga kontrolluesi, që janë në

спроведување на техничките и организациските мерки за обезбедување безбедност на обработката на личните податоци согласно прописите за заштита на личните податоци;	funksion të zbatimit të masave teknike dhe organizative për të siguruar sigurinë e përpunimit të të dhënave personale në përputhje me dispozitat e mbrojtjes së të dhënave personale;
9. **Авторизиран пристап** е овластување доделено на овластеното лице за обработка на личните податоци, за користење на одредена информатичко комуникациска опрема или за пристап до одредени работни простории на контролорот;	9. **Qasja e autorizuar** është autorizimi që i jepet personit të autorizuar për përpunimin e të dhënave personale, për përdorimin e pajisjeve të caktuara të informacionit dhe komunikimit ose për qasje në hapësira të caktuara të punës së kontrolluesit;
10. **Администратор на информацискиот систем** е лице овластено за планирање и за применување на технички и организациски мерки, како и за контрола на обезбедувањето тајност и заштита на обработката на личните податоци;	10. **Administratori i sistemit të informacionit** është personi i autorizuar për planifikimin dhe zbatimin e masave teknike dhe organizative, si dhe për kontrollin e sigurimit të fshehtësisë dhe mbrojtjen e përpunimit të të dhënave personale;
11. **Документ** е секој запис кој содржи лични податоци и истиот може да биде во електронска или хартиена форма, да се чува на медиум и во информатичко комуникациската опрема која се користи за обработка на податоците, да се доставува преку пошта или да се пренесува преку електронско комуникациска мрежа.	11. **Dokument** është çdo shkresë që përmban të dhëna personale dhe mund të jetë në formë elektronike dhe në letër, të ruhet në media dhe në pajisje informatike komunikimi që përdoret për përpunimin e të dhënave, të dorëzohet nëpërmjet postës apo të bartet nëpërmjet rrjetit elektronik të komunikimit.
12. **Информатичка инфраструктура** е целата информатичко комуникациска опрема на контролорот, во рамките на која се собираат, обработуваат и чуваат личните податоци;	12. **Infrastruktura e informacionit** është e tërë pajisja e informacionit dhe komunikimit e kontrolluesit, brenda së cilës mblidhen, përpunohen dhe ruhen të dhënat personale;
13. **Информациски систем** е систем со кој може да се обработуваат личните податоци со цел да бидат достапни и употребливи за секој кој што има право и потреба да ги користи;	13. **Sistemi i informacionit** është një sistem me të cilin mund të përpunohen të dhënat personale në mënyrë që të jenë të kapshme dhe të përdorshme për këdo që ka të drejtë dhe nevojë për t'i përdorur ato;
14. **Инцидент** е секоја аномалија која влијае или може да влијае на тајноста и заштитата на личните податоци;	14. **Incident** është çdo anomali që ndikon apo mund të ndikojë në fshehtësinë dhe mbrojtjen e të dhënave personale;

15. **Контрола на пристап** е операција за доделување на пристап до личните податоци или до информатичко комуникациската опрема со цел проверка на овластеното лице;	15. **Kontrolli i qasjes** është operacion për ndarjen e qasjes në të dhënat personale ose pajisjet e informacionit dhe komunikimit për të kontrolluar personin e autorizuar;
16. **Овластено лице** е лице вработено или ангажирано кај контролорот кое има авторизиран пристап до документите и до информатичко комуникациската опрема на кои се обработуваат лични податоци;	16. **Personi i autorizuar** është një person i punësuar ose i angazhuar te kontrolluesi i cili ka qasje të autorizuar në dokumente dhe pajisjen e informacionit dhe komunikimit, në të cilat përpunohen të dhënat personale;
17. **Лозинка** е доверлива информација составена од множество на карактери кои се користат за проверка и автентикација на овластеното лице;	17. **Fjalëkalimi** është informacion i besueshëm i përbërë nga një grup karakteresh që përdoren për të kontrolluar dhe autentifikuar personin e autorizuar;
18. **Колаче (cookie)** е информација која што се креира и испраќа од веб-серверот до веб пребарувачот, а која потоа се испраќа назад, како непроменета информација од веб-пребарувачот секогаш кога повторно ќе се пристапи до веб-серверот кој ја креирал информацијата.	18. **Biskota (cookie)** është informacioni që krijohet dhe dërgohet nga serveri i faqes deri te shfletuesi i faqes, e që më pas dërgohet përsëri, si informacion i pandryshuar nga shfletuesi i faqes sa herë që ka qasje përsëri në serverin e faqes që e ka krijuar informacioni.
19. **Работна станица** е секој уред (десктоп, лаптоп) кој поврзан во мрежа претставува дел од опремата на контролорот, а на кој, односно со кој се врши обработка на личните податоци во информацискиот систем;	19. **Stacion i punës** është çdo pajisje (desktop, laptop) që i lidhur me rrjet paraqet pjesë të pajisjes së kontrolluesit, e në të cilën përkatësisht me të cilën përpunohen të dhënat personale në sistemin e informacionit;
20. **Медиум** е физички уред кој се користи при обработка на личните податоци во информацискиот систем, на кој податоците можат да бидат снимени или од кој истите можат да бидат повторно вратени; и	20. **Media** është një pajisje fizike që përdoret gjatë përpunimit të të dhënave personale në sistemin e informacionit, në të cilën mund të regjistrohen të dhënat ose nga i cili mund të kthehen përsëri; dhe
21. **Сигурносна копија** е копија на личните податоци содржани во електронските документи, кои се зачувани на медиум за да се овозможи нивно повторно враќање.	21. **Kopje sigurie** është kopje e të dhënave personale që i përmbajnë dokumentet elektronike, të cilat ruhen në media për të mundësuar rikthimin e tyre.

Примена	Zbatimi
Член 3	**Neni 3**
Одредбите од овој правилник се применуваат и при обработка на личните податоци од страна на обработувачот на збирка на лични податоци.	Dispozitat e kësaj rregulloreje zbatohen gjithashtu edhe gjatë përpunimit të të dhënave personale nga përpunuesi i përmbledhjes së të dhënave personale.
Одржување на информацискиот систем	**Mirëmbajtja e sistemit të informacionit**
Член 4	**Neni 4**
(1) Физичките или правните лица кои вршат одржување на информацискиот систем на контролорот треба да ги применуваат прописите за заштита на личните податоци и донесената документација за технички и организациски мерки.	(1) Personat fizikë ose juridikë që mirëmbajnë sistemin e informacionit të kontrolluesit duhet t'i zbatojnë dispozitat për mbrojtjen e të dhënave personale dhe dokumentacionin e miratuar për masat teknike dhe organizative.
(2) Одредбите од ставот (1) на овој член се применуваат и ако физичките или правните лица вршат обработка на личните податоци на контролорот.	(2) Dispozitat e paragrafit (1) të këtij neni zbatohen gjithashtu edhe nëse personat fizikë ose juridikë përpunojnë të dhënat personale të kontrolluesit.
Пренос на лични податоци во трети земји	**Transferimi i të dhënave personale në vendet e treta**
Член 5	**Neni 5**
Во случај на хардверско и/или софтверско одржување или на други активности на информацискиот систем може да се врши пренос на лични податоци во трети земји само согласно условите утврдени во прописите за заштита на личните податоци.	Në rast të mirëmbajtjes së harduerit dhe/ose softuerit ose aktiviteteve të tjera të sistemit të informacionit, të dhënat personale mund të transferohen në vendet e treta vetëm në përputhje me kushtet e përcaktuara në dispozitat për mbrojtjen e të dhënave personale.
II. БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ	**II. SIGURIA E PËRPUNIMIT TË TË DHËNAVE PERSONALE**
Систем за заштита на личните податоци	**Sistemi i mbrojtjes së të dhënave personale**
Член 6	**Neni 6**
(1) Според најновите технолошки достигнувања, трошоците за спроведување и	(1) Sipas arritjeve të fundit teknologjike, shpenzimet e zbatimit dhe natyra, fushëveprimi, konteksti i

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.	përpunimit, si dhe rreziqet me shkallë të ndryshme të probabilitetit dhe serioziteti për të drejtat dhe liritë e personave fizikë, kontrolluesi është i obliguar të vendosë sistem për mbrojtjen e të dhënave personale nëpërmjet zbatimit të teknikave përkatëse dhe masave organizative për të siguruar nivel sigurie, të përshtatshëm me rrezikun.
(2) Техничките и организациските мерки од ставот (1) на овој член, особено опфаќаат:	(2) Masat teknike dhe organizative nga paragrafi (1) i këtij neni, përfshijnë sidomos:
- псевдонимизација и криптирање на личните податоци;	- pseudonimizim dhe kriptim të të dhënave personale;
- способност за обезбедување на континуирана доверливост, интегритет, достапност и отпорност на информацискиот систем за обработка;	- aftësia për të siguruar besueshmëri të vazhdueshme, integritet, disponueshmëri dhe rezistencë të sistemit të përpunimit të informacionit;
- способност за навремено, повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на физички или технички инцидент; и	- aftësi për rivendosje në kohë të qasjes në të dhënat personale dhe qasjen në to në rast të ndonjë incidenti fizik ose teknik; dhe
- процес на редовно тестирање, оценување и евалуација на ефективноста на техничките и организациските мерки со цел да се гарантира безбедноста на обработката.	- proces i testimit të rregullt, vlerësimit dhe evaluimit të rregullt të efektivitetit të masave teknike dhe organizative, që të garantohet siguria e përpunimit.
(3) 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*).	(3) Kontrolluesi vlerëson dhe përditëson masat teknike dhe organizative dhe zbaton gjithnjë ato masa që janë të përshtatshme për kohën në të cilën ato dizajnohen dhe zbatohen, dhe në përputhje me arritjet e fundit teknologjike *(a state of the art technology).*
(4) Процесот за управување со системот за заштита на личните податоци од ставот (1) на овој член 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	(4) Procesi për menaxhim me sistemin për mbrojtjen e të dhënave personale nga paragrafi (1) i këtij neni përcaktohet në Politikën për sistemin e mbrojtjes së të dhënave personale të kontrolluesit i cili duhet të korrespondojë me natyrën, fushën dhe kompleksitetin e veprimtarive që kontrolluesi kryen gjatë përpunimit të të dhënave personale dhe

ризиците на коишто е изложен.	rreziqet ndaj të cilave ekspozohet.
(5) Контролорот е должен Политиката од ставот (4) на овој член да ја ревидира и усогласува согласно промените во неговото работење.	(5) Kontrolluesi është i detyruar të rishikojë dhe të harmonizojë Politikën nga paragrafi (4) i këtij neni në përputhje me ndryshimet në funksionimin e tij.
Управување со ризик	**Menaxhimi i rrezikut**
Член 7	**Neni 7**
(1) 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.	(1) Kontrolluesi gjatë përcaktimit dhe vlerësimit të rrezikut (menaxhimi i rrezikut) duhet të marrë parasysh rreziqet që lidhen me përpunimin, sidomos nga shkatërrimi i rastësishëm ose i paligjshëm, humbjes, ndryshimit, zbulimit të paautorizuar të të dhënave personale ose qasjes së paautorizuar deri te të dhënat personale të transmetuara, të ruajtura ose të përpunuara në mënyrë tjetër.
(2) Управувањето со ризикот од ставот (1) на овој член ги опфаќа следните фази:	(2) Menaxhimi i rrezikut nga paragrafi (1) i këtij neni, përfshin këto fazat:
а) список (преглед) на сите процеси со кои се врши обработка на лични податоци;	a) lista (rishikim) e të gjitha proceseve me të cilat kryhet përpunimi i të dhënave personale;
б) процена на ризиците за секој процес на обработка на лични податоци;	b) vlerësimi i rreziqeve për çdo proces të përpunimit të të dhënave personale;
в) спроведување и проверка на планираните мерки; и	c) zbatimi dhe verifikimi i masave të planifikuara; dhe
г) спроведување на периодични безбедносни проверки.	ç) zbatimi i kontrolleve periodike të sigurisë.
(3) Списокот на процеси со кои се врши обработка на личните податоци од став (2) точка а) на овој член преку целосно или делумно автоматизирана обработка на личните податоци или друга обработка на лични податоци, треба најмалку да ги опфати:	(3) Lista e proceseve me të cilat përpunohen të dhënat personale nga paragrafi (2) pika a) e këtij neni nëpërmjet përpunimit plotësisht të automatizuar ose pjesërisht të të dhënave personale ose përpunimit tjetër të të dhënave personale, duhet të paktën të përfshijë:
хардверот (на пример: сервери, лаптопи,	hardueri (për shembull: serverë, laptopë, hard

хард дискови и други медиуми);	disqe dhe media të tjera);
софтверот (на пример: оперативни системи и софтверски програми развиени за потребите на контролорот);	softueri (për shembull: sistemet operative dhe programe softuerike, të zhvilluara për nevojat e kontrolluesit);
комуникациски канали (на пример: оптички кабли, интернет, безжична мрежна технологија – Wi-Fi);	kanale komunikimi (për shembull: kabllo optik, internet, teknologji rrjeti pa kabllo- Wi-Fi);
- документи во хартиена форма (на пример: печатени документи, фотокопии).	- dokumente në formë të shkruar (për shembull: dokumente të shtypura, fotokopje).
- (4) Проценатa на ризиците од став (2) точка б) на овој член, треба најмалку да ги опфати:	- (4) Vlerësimi i rreziqeve nga paragrafi (2) pika 6) nga ky nen, duhet t'i përfshijë:
- (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:	- (a) vërtetimi i ndikimeve dhe efekteve potenciale mbi të drejtat dhe liritë e personave fizikë të cilëve u referohet edhe atë për kërcënimet potenciale si në vijim, përkatësisht situatat:
- неовластен пристап до личните податоци;	- qasje të paautorizuar në të dhënat personale;
непосакувани промени на личните податоци; и	ndryshime të padëshiruara në të dhënat personale; dhe
привремена или целосна недостапност до личните податоци.	paqasshmëri e përkohshme ose e plotë deri te të dhënat personale.
- (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	- b) identifikimi i burimeve të rrezikut që mund të jenë shkak i ndonjë ngjarjeje të padëshiruar, kurse duke marrë parasysh burimet njerëzore të brendshme dhe të jashtme (për shembull: administratori i sistemit të informacionit, personi i autorizuar, sulmuesi i jashtëm, konkurrenti), si dhe burime të tjera të brendshme dhe të jashtme (p.sh. uji, materialet e rrezikshme, zjarri, virusi).

(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:	- c) identifikimi i kërcënimeve të mundshme që mund të ndodhin nëpërmjet mediave nga të cilat varen të dhënat personale (për shembull: harduer, softuer, kanale komunikimi, dokumente në formë letre etj.), e të cilat mund të jenë:
- употребени на несоодветен начин (на пример: злоупотреба на овластувањата, грешка при ракување);	- të përdorura në mënyrë të papërshtatshme (për shembull: shpërdorimi i autorizimeve, gabime gjatë dorëzimit;
изменети (на пример: „заразен" софтвер или хардвер – keylogger, инсталирање на злонамерен софтвер, итн);	të ndryshuara (për shembull: softuer ose harduer "i infektuar" - keylogger, instalimi i softuerit malicioz etj.);
изгубени (на пример: кражба на лаптоп или губење на мемориски уред – УСБ);	të humbura (për shembull: vjedhje të laptopit ose humbja e pajisjes së memories – USB);
- набљудувани (на пример: гео-локација на опремата);	- të vëzhguara (për shembull: gjeo-lokacioni i pajisjes);
- оштетени (на пример: вандализам, деградација заради природно абење);	- të dëmtuara (për shembull: vandalizëm, degradim për shkak të harxhimit natyral);
- преоптоварени (на пример: медиумот за складирање е целосно пополнет, denial of service attack и сл.).	- të mbingarkuara (për shembull: mediumi për grumbullim është plotësisht e mbushur, denial of service attack etj.)
- (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).	- (ç) Vërtetim të masave ekzistuese ose të planifikuara që mundësojnë zgjidhjen e çdo rreziku (për shembull: kontrolli i hyrjes, kopje sigurie, gjurmët e kontrollit të informacionit, siguria e hapësirave, kriptimi ose anonimizimi).
- (д) Оценување на сериозноста и веројатноста на ризиците, во однос	- (d) Vlerësimi i seriozitetit dhe probabilitetit të rreziqeve, në lidhje

на претходните елементи предвидени во овој став (на пример: скала што може да се користи за проценка: занемарлива, умерена, значајна и максимална).	me elementët e mëparshëm të parashikuar në këtë paragraf (për shembull: shkallë që mund të përdoret për vlerësim: neglizhuese, mesatare, e rëndësishme dhe maksimale).
- (5) Контролорот задолжително врши спроведување и проверка на планираните мерки од став (2) точка в) на овој член, а со цел да се обезбеди дека тие се применуваат и тековно се тестираат.	- (5) Kontrolluesi doemos kryen zbatimin dhe kontrollimin e masave të planifikuara nga paragrafi (2) pika c) të këtij neni, me qëllim që të sigurohet se ato zbatohen dhe testohen vazhdimisht.
(6) Контролорот задолжително спроведува периодични безбедносни проверки од став (2) точка г) на овој член, за што се подготвува акционен план, чија имплементација се следи од страна на раководството на контролорот.	(6) Kontrolluesi doemos kryen kontrolle periodike të sigurisë nga paragrafi (2) pika ç) të këtij neni, për të cilin përgatitet plan veprimi, zbatimi i të cilit vëzhgohet nga kryesia e kontrolluesit.
Нивоа на мерки за безбедност на обработката на личните податоци	**Nivelet e masave të sigurisë për përpunimin e të dhënave personale**
Член 8	**Neni 8**
(1) 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.	(1) Duke marrë parasysh natyrën, vëllimin, kontekstin dhe objektivat e përpunimit, si dhe rreziqet me probabilitet të ndryshëm dhe seriozitet të të drejtave dhe lirive të personave fizikë, kontrolluesi është i obliguar të zbatojë nivel të duhur të masave teknike dhe organizative që do të jenë proporcionale me aktivitetet për përpunimin e të dhënave personale.
(2) Техничките и организациските мерки од ставот (1) на овој член се класифицираат во две нивоа:	(2) Masat teknike dhe organizative nga paragrafi (1) i këtij neni klasifikohen në dy nivele:
стандардно; и	standarde; dhe
високо.	të larta
(3) Во согласност со ставот (1) од овој член, контролорот кој обработува лични податоци за помалку од 10 вработени како единствена збирка на лични податоци, нема обврска да	(3) Në përputhje me paragrafin (1) të këtij neni, kontrolluesi që përpunon të dhëna personale për më pak se 10 punonjës si një përmbledhje e vetme e të dhënave personale, nuk ka për

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.	obligim të zbatojë masa teknike dhe organizative, përveç nëse ka mundësi se përpunimi i kryer paraqet rrezik për të drejtat dhe liritë e subjekteve të të dhënave personale, nëse përpunimi nuk është i përkohshëm apo përpunimi përfshin kategori të veçanta të të dhënave personale ose të dhëna personale që lidhen me gjykime dhe veprat penale.
-	-
- **Примена на нивоа на мерки за безбедност на обработката на личните податоци**	- **Zbatimi i niveleve të masave të sigurisë për përpunimit e të dhënave personale**
Член 9	**Neni 9**
(1) Контролорот е одговорен за усогласеноста во однос на нивото на мерки за безбедност на обработката на личните податоци кое ќе го примени во согласност со членот 8 од овој правилник, при што треба да обезбеди соодветно ниво на безбедност на личните податоци, вклучувајќи заштита од неовластена или незаконска обработка, како и заштита од нивно случајно губење, уништување или оштетување.	(1) Kontrolluesi është përgjegjës për përshtatjen me nivelin e masave të sigurisë për përpunimin e të dhënave personale të cilat ai do t'i zbatojë në përputhje me nenin 8 të këtij rregulli, ku duhet të sigurojë nivel përkatës të sigurisë së të dhënave personale, përfshirë mbrojtjen nga përpunimi i paautorizuar ose i paligjshëm, si dhe mbrojtje nga humbja e rastësishme, shkatërrimi apo dëmtimi.
(2) Контролорот ја демонстрира примената на мерките според барањата утврдени во ставот (1) на овој член, вклучувајќи ги причините и основите за изборот на примената на стандардното, односно високото ниво.	(2) Kontrolluesi demonstron zbatimin e masave sipas kërkesave të përcaktuara në paragrafin (1) të këtij neni, duke përfshirë bazat dhe arsyet e zgjedhjes së zbatimit të standardit, përkatësisht nivelin e lartë.
III. СТАНДАРДНО НИВО	**III. NIVELI STANDARD**
Документација за технички и организациски мерки	**Dokumentacion për masat teknike dhe organizative**
Член 10	**Neni 10**
(1) Контролорот во Политиката за системот за заштита на личните податоци ги утврдува и начелата за безбедност и заштита на личните податоци.	(1) Kontrolluesi në Politikën për sistemin e mbrojtjes së të dhënave personale i vërteton parimet për sigurinë dhe mbrojtjen e të dhënave personale.
(2) 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	(2) Bazuar në Politikën për sistemin e mbrojtjes së të dhënave personale, kontrolluesi miraton politika dhe procedura më të hollësishme, ku

овластените лица кои имаат пристап до личните податоци и до информацискиот систем и информатичка инфраструктура.	përshkruhen masat teknike dhe organizative për personat e autorizuar që kanë qasje deri te të dhënat personale dhe deri në sistemin e informacionit dhe infrastrukturën e informacionit.
(3) Документираните процеси од ставот (2) на овој член особено се однесуваат на:	(3) Proceset e dokumentuara nga paragrafi (2) i këtij neni kanë të bëjnë me:
идентификацијата, оценката и класификацијата на ризикот на процесите со кои се врши обработка на личните податоци (анализа на ризик);	identifikimin, vlerësimin dhe klasifikimin e rrezikut të proceseve me të cilat përpunohen të dhënat personale (analiza e rrezikut);
општ опис на техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци соодветно на ризикот;	përshkrimin e përgjithshëm të masave teknike dhe organizative për të siguruar fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale në përputhje me rrezikun;
активности за обука и подигнување на свеста на раководството и вработените за приватноста и безбедносните ризици во контролорот;	aktivitete për trajnim dhe ngritje të vetëdijes së udhëheqjes dhe të punësuarve lidhur me privatësinë dhe rreziqet e sigurisë së kontrolluesit;
- 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);	- dizajnimin, zhvillimin dhe mirëmbajtjen e programeve softuerike për përpunimin e të dhënave personale, e sidomos në drejtim të mbrojtjes teknike dhe të integruar të të dhënave personale (Data protection by design and by default);
- начинот на обезбедување на автентикација на овластените лица во информацискиот систем;	- mënyra e sigurimit të autentifikimit për personat e autorizuar në sistemin e informacionit;
- начинот на обезбедување на контрола на пристап до информацискиот систем;	- mënyrën e sigurimit të kontrollit të qasjes në sistemin e informacionit;
- начинот на обезбедување евиденција за секој пристап до информацискиот систем (на пример до: оперативните системи, заштитниот ѕид (firewall), серверот дизајниран специјално за употреба како сервер за датотеки (file	- mënyrën e sigurimit të evidencës për secilën qasje në sistemin e informacionit (për shembull te: sistemet operative, muri mbrojtës firewall), serveri i dizajnuar posaçërisht për t'u përdorur si server i datotekës (file server), bazat e të

server), базите на податоци, системот (софтверот) за управување со документи (DMS System), софтверот за управување со врски со клиенти (CRM Software) и сл.);	dhënave, sistemi (softueri) për menaxhim me dokumente (DMS System), softueri për menaxhimin e lidhjeve me klientët (CRM Software), etj.);
- начинот на управување со инциденти (инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци);	- mënyrën e menaxhimit me incidente (incidente që e rrezikojnë besueshmërinë, integritetin apo qasjen deri te të dhënat personale);
- начинот на обезбедување на опремата на контролорот на која се врши обработка на личните податоци;	- mënyrën e sigurimit të pajisjes së kontrolluesit në të cilën bëhet përpunimi i të dhënave personale;
- начинот на обезбедување на преносливите медиуми;	- mënyrën e sigurimit të mediave portative;
- начинот на заштита на внатрешната мрежа на контролорот;	- mënyrën e mbrojtjes së rrjetit të brendshëm të kontrolluesit;
- начинот на обезбедување на серверите и веб-страницата на контролорот;	- mënyrën e sigurimit të serverëve dhe uebfaqen e kontrolluesit;
- начинот на евидентирање и чување на документацијата за софтверските програми за обработка на личните податоци;	- mënyrën e evidentimit dhe ruajtës së dokumentacionit për programet softuerike për përpunimin e të dhënave personale;
- начинот на обработка на личните податоци кои се псевдонимизирани;	- mënyrën e përpunimit të të dhënave personale që janë të pseudonimizuara;
- начинот на обработка на личните податоци кои се криптирани;	- mënyrën e përpunimit të të dhënave personale që janë të kriptuara;
- обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема;	- obligimet dhe përgjegjësitë e administratorit të sistemit të informacionit dhe personave të autorizuar gjatë përdorimit të dokumenteve dhe pajisjeve të informacionit dhe komunikimit;
- начинот и процесите за пријавување, реакција и санирање на инциденти;	- mënyrën dhe procesin për paraqitje, reagim dhe zgjidhjen e incidenteve;
- начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните	- mënyrën e bërjes së kopjes, arkivim dhe ruajtje, si dhe për kthim të sërishëm të të dhënave të ruajtura personale;

лични податоци;	
- начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите;	- mënyrën e shkatërrimit të dokumenteve, si dhe për mënyrën e shkatërrimit, fshirjes dhe pastrimit të mediave;
- физичка безбедност;	- sigurinë fizike;
- начинот на ангажирање и контрола на надворешни субјекти (обработувачи);	- mënyrën e angazhimit dhe kontrollit të subjekteve të jashtme (përpunues);
- динамика и начин на вршење на периодични контроли, како и процесите за вршење на внатрешна контрола; и	- dinamikën dhe mënyrën e kryerjes së kontrolleve periodike si dhe proceset për kryerjen e kontrollit të brendshëm; dhe
- други мерки кои контролорот ги применува врз основа на анализата на ризикот.	- Masa të tjera që kontrolluesi i zbaton në bazë të analizës së rrezikut.
- (4) Документацијата од ставовите (2) и (3) на овој член, 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.	- (4) Dokumentacionin nga paragrafët (2) dhe (3) të këtij neni, kontrolluesi e ndryshon dhe e plotëson në rast të ndryshimeve në sistemin informatik dhe të infrastrukturës informatike, ndërsa të paktën një herë në vit, bën vlerësimin, evaluimin dhe përditësimin e tij.
-	-
- **1. Технички мерки**	- **1. Masat teknike**
Автентикација на овластените лица	**Autentifikimi i personave të autorizuar**
Член 11	**Neni 11**
(1) Контролорот обезбедува најавата во информацискиот систем да се врши преку единствен идентификатор кој се поврзува само со едно овластено лице.	(1) Kontrolluesi siguron që njoftimi në sistemin e informacionit të bëhet nëpërmjet një identifikuesi të vetëm që është i lidhur vetëm me një person të autorizuar.
(2) Во согласност со ставот (1) од овој член единствениот идентификатор контролорот може да го обезбеди преку:	(2) Në përputhje me paragrafin (1) të këtij neni, identifikuesin e vetëm kontrollori mund ta sigurojë nëpërmjet:
информација која единствено овластеното	informacionit që vetëm personi i autorizuar e

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;	din (për shembull: emrin e vetëm të përdoruesit dhe fjalëkalimin për çdo person të autorizuar, ku fjalëkalimi duhet të përbëhet nga kombinimi i të paktën tetë shkronjave të karaktereve alfa numerike (të vogla dhe të mëdha), simboleve, numrave dhe shenjave të pikësimit;
нешто што само овластеното лице го поседува (на пример: паметна картичка – smart card);	diçka që vetëm personi i autorizuar e posedon (për shembull: kartelë të mençur- smart card);
нешто што овластеното лице е, или го прави (на пример: дигитален потпис); и	diçka që personi i autorizuar është apo e bën (për shembull: nënshkrim digjital); dhe
- 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.	- mënyrave të tjera të autentifikimit që sipas arritjeve të fundit teknologjike, e në kontekstin e analizës së kryer të rrezikut, sigurojnë identifikues të vetëm që lidhet vetëm me një person të autorizuar.
- (3) Автентикацијата на овластените лица, контролорот ја врши најмалку преку еден од наведените начини од ставот (2) на овој член. 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).	- (3) Autentifikimin e personave të autorizuar, kontrolluesi e kryen të paktën me një nga mënyrat e përcaktuara nga paragrafi (2) i këtij neni. Në varësi të analizës së rrezikut, për persona të caktuar të autorizuar ose për të gjithë, mund të përdoret një kombinim i dy ose më shumë faktorëve të autentifikimit (për shembull: emrin e vetëm përdoruesit dhe fjalëkalimin në kombinim me përdorimin e një kartele të mençur).
- (4) Контролорот задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и	- (4) Kontrolluesi në mënyrë të obliguar duhet të mbajë evidencë për personat e autorizuar që kanë qasje të autorizuar në dokumente dhe

информацискиот систем, како и воспоставува постапки за идентификација и проверка на авторизираниот пристап.	sistemin e informacionit, si dhe të vendosë procedura për identifikimin dhe verifikimin e qasjes së autorizuar.
- (5) 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.	- (5) Kur kontrolli kryhet në bazë të emrit të përdoruesit dhe fjalëkalimit, kontrollori duhet t'i zbatojë gjithmonë rregullat që garantojnë besueshmërinë dhe integritetin e tyre gjatë lajmërimit, ndarjes dhe ruajtjen e tyre, ku fjalëkalimet në mënyrë të obligueshme ndryshohen automatikisht pas një kohe të caktuar në bazë të analizës së rrezikut, që nuk mund të jetë më e gjatë se tre muaj.
Обезбедување на опремата на која се врши обработка на личните податоци	**Sigurimi i pajisjes në të cilën përpunohen të dhënat personale**
Член 12	**Neni 12**
(1) Контролорот е должен да обезбеди примена на технички мерки со кои се обезбедува опремата на која се врши обработка на личните податоци и тоа:	(1) Kontrolluesi është i obliguar të sigurojë zbatimin e masave teknike me të cilat sigurohen pajisjet në të cilat kryhet përpunimi i të dhënave personale, edhe atë:
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 согласност со член 11 од овој правилник;	çlajmërim i automatizuar nga sistemi i informacionit pas një periudhe të caktuar të pasivitetit (jo më shumë se 15 minuta). Për të riaktivizuar sistemin, kontrolluesi duhet të sigurojë që personat e autorizuar qasen duke zbatuar autentifikimin sipas nenit 11 të kësaj Rregullore;
во случај на одреден број на неуспешни обиди за најавување на информацискиот	në rast të një numri të caktuar të përpjekjeve të pasuksesshme për t'u lajmëruar në sistemin e

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;	informacionit, që janë në kundërshtim me politikat e autentifikimit të kontrolluesit, duhet të sigurohet refuzim i automatizuar nga sistemi i informacionit. Numri i përpjekjeve të pasuksesshme përcaktohet nga kontrolluesi sipas rrezikut dhe natyrës së punës dhe proceseve të punës lidhur me përpunimin e të dhënave personale, por jo më shumë se pesë përpjekje të njëpasnjëshme të pasuksesshme;
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;	mur mbrojtës i instaluar (firewall) dhe kufizim të portave të autorizuara për komunikimin e atyre që janë rreptësisht të domosdoshëm për funksionimin e duhur të programeve softuerike të instaluar në vendet e punës të kontrolluesit;
- редовно ажуриран антивирусен софтвер и дефинирана политика за редовни ажурирања на софтверските програми;	- softuer i rregullt i përditësuar kundër virusit dhe politikave të përkufizuara për përditësime të rregullta të programeve softuerike;
- конфигурирани софтверски програми така што безбедносните ажурирања да се вршат автоматски;	- programe të konfiguruara softuerike, që përditësimet e sigurisë të kryhen automatikisht;
- 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;	- ruajtje të informacioneve të shfrytëzuesve të serverëve të kontrolluesit për të cilat rregullisht bëhet kopje të sigurisë, ndërsa në rastet kur informacionet ruhen në mënyrë lokale, në mënyrë të obliguar me masat për sinkronizim apo me masat plotësuese rezervë për mbrojtjen në bazë të analizës së rrezikut;
- ограничување на опцијата за приклучување на преносливите медиуми (УСБ, надворешни хард дискови и сл.) кон системите со примарна важност;	- kufizim i opsionit për kyçje të mediave portative (USB, hard disqe të jashtme, etj.) ndaj sistemeve me rëndësi parësore;

- исклучен автоматски режим на работа за преносливите медиуми (Disable autorun for removable media);	- regjim i çkyçur automatik i punës për media portative (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;	- veglat e administrimit në distancë duhet të vendosen në atë mënyrë që ata paraprakisht të sigurojnë pëlqimin e përdoruesit (personit të autorizuar) të stacionit të punës para çdo intervenimi të vet stacionit të punës;
- 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	- rregullimi i sistemit të informacionit që do të sigurojë se përdoruesi (personi i autorizuar) në stacionin e punës mund të vërejë nëse kryhet administrimi nga larg, si dhe kur ka përfunduar i njëjti (për shembull duke shfaqur mesazh në ekran se administrata nga larg ka mbaruar); dhe
- приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.	- lidhje të sistemit të informacionit (kompjuterët dhe serverët) me rrjetin energjetik nëpërmjet pajisjes për furnizimin e pandërprerë me energji.
- (2) Покрај мерките од ставот (1) на овој член, врз основа на спроведената анализа на ризик, доколку се утврди за потребно, контролорот ги применува и следните мерки:	- (2) Krahas masave nga paragrafi (1) i këtij neni, në bazë të analizës së zbatuar të rrezikut, nëse vërtetohet si e nevojshme, kontrolluesi i zbaton edhe këto masa:
- забрана на работа со преземени софтверски програми кои не доаѓаат од безбедни извори;	- ndalesë të punës me programe të ndërmarra softuerike që nuk vijnë nga burime të sigurta;
- ограничување на употребата на софтверски програми што бараат	- kufizim të përdorimit të programeve softuerike që kërkojnë të drejta të

администраторски права;	administratorit;
бришење на податоците што се наоѓаат на работна станица која треба да се предаде;	fshirje të informacioneve që gjenden në stacionin e punës që duhet të dorëzohet;
- 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;	- në rast se stacioni i punës është i kompromentuar, verifikim i obligueshëm dhe sipas mundësisë të gjendet burimi, si dhe çdo gjurmë e ndërhyrjes në sistemin e informacionit të kontrolluesit, në mënyrë që të zbulohet nëse janë të rrezikuara elementet e tjera;
- безбедносен надзор на софтверот и хардверот што се користи во системот на контролорот, вклучувајќи и редовно следење на тимот за брза реакција (МКD-CIRT) во однос на неговите предупредувања и совети за ранливости откриени во софтверот и хардверот;	- monitorim sigurie të softuerit dhe harduerit që përdoret në sistemin e kontrolluesit, përfshirë edhe ndjekjen e rregullt të ekipit për reagim të shpejtë (MKD-CIRT) në lidhje me paralajmërimet e tij dhe këshillat e rreziqeve të zbuluara në softuer dhe harduer;
- ажурирање на софтверските програми кога се идентификуваат и ги коригираат критичните недостатоци;	- përditësimi i programeve softuerike kur identifikohen dhe korrigjohen mungesat kritike;
- инсталирање на ажурирања на оперативните системи со автоматска верификација согласно проценатa на ризик, а најмалку еднаш неделно; и	- instalimi i përditësimeve në sistemet operative me verifikim automatik sipas vlerësimit të rrezikut, të paktën një herë në javë; dhe
- 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.	- ngritjen e nivelit të ndërgjegjësimit në lidhje me atë, që personat e autorizuar duhet të përkushtohen dhe të dhënat e kontaktit të personave me të cilët duhet të kontaktojnë në rast të ndonjë incidenti ose paraqitjes së ndonjë ngjarjeje të pazakontë që ndikon ndaj informacioneve dhe komunikimin e sistemeve të kontrolluesit.
Сегрегација на должности и одговорности	**Ndarja e detyrimeve dhe përgjegjësive**
Член 13	**Neni 13**
(1) Контролорот ги утврдува овластените	(1) Kontrolluesi përcakton personat e

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.	autorizuar që duhet të kenë qasje në sistemin e informacionit, ku siguron ndarje të qarta të detyrave dhe përgjegjësive sipas rregullit "është e nevojshme të dihet" përkatësisht se personi i autorizuar do të ketë qasje vetëm në ato të dhëna personale që janë të nevojshme për kryerjen e detyrave të tyre.
(2) Контролорот обезбедува повлекување на правата на пристап веднаш по престанокот на овластувањата за пристап.	(2) Kontrolluesi siguron tërheqjen e të drejtave të qasjes menjëherë pas përfundimit të autorizimeve të hyrjes.
(3) 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.	(3) Kontrolluesi kontrollon dhe përditëson privilegjet për qasje në sistemin e informacionit të personave të autorizuar. Verifikimi kryhet për periudha që përcaktohen në bazë të analizës së rrezikut, të paktën në nivel tremujor.
Контрола на пристап до информацискиот систем	**Kontrolli i qasjes në sistemin e informacionit**
Член 14	**Neni 14**
(1) Овластените лица задолжително имаат авторизиран пристап само до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работни задачи.	(1) Personat e autorizuar në mënyrë të obliguar kanë qasje të autorizuar vetëm në të dhënat personale dhe pajisjet e komunikimit dhe informacionit që janë të domosdoshme për kryerjen e detyrave të tyre të punës.
(2) Контролорот воспоставува механизми за да се оневозможи пристап на овластените лица до личните податоци и информатичко комуникациската опрема со права различни од тие за кои се авторизирани.	(2) Kontrolluesi vendos mekanizma dhe e bën të pamundur qasjen e personave të autorizuar në të dhënat personale dhe pajisjet informatike të komunikimit me të drejta të ndryshme nga ato për të cilat janë të autorizuar.
(3) 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	(3) Administratori i sistemit të informacionit që është i autorizuar nga kontrolluesi, ndan, ndryshon ose merr privilegjet e qasjes së autorizuar në të dhënat personale dhe pajisjet e komunikimit dhe informacionit vetëm në përputhje me kriteret e përcaktuara nga

согласност со критериумите кои се утврдени од страна на контролорот.	kontrolluesi.
Обезбедување евиденција за секој пристап (logs)	**Sigurim të evidencës për çdo qasje (logs)**
Член 15	**Neni 15**
(1) 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 ѕид (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;	(1) Me qëllim që të sigurojë identifikimin e çdo qasjeje të paautorizuar (mashtrues) ose keqpërdorim të të dhënave personale, si dhe për të përcaktuar prejardhjen e këtyre incidenteve, kontrolluesi vendos dhe mban shënime për çdo qasje në sistemin e informacionit - logs (për shembull: nga sistemet operative, nga muri mbrojtës (firewall), serveri i dizajnuar posaçërisht për t'u përdorur si server i datotekave (file server), bazat e të dhënave, sistemi (softueri) për rregullimin e dokumenteve (DMS System), softueri i menaxhimit në lidhje me klientë (CRM Software) etj.;
(2) Евиденцијата од ставот (1) на овој член треба да ги содржи особено следните податоци: име и презиме на овластеното лице, работната станица од каде се пристапува до информацискиот систем, датум и време на пристапување, лични податоци кон кои е пристапено, видот на пристапот со операциите кои се преземени при обработка на податоците, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.	(2) Evidenca nga paragrafi (1) i këtij neni duhet t'i përmbajë të dhënat e mëposhtme: emrin dhe mbiemrin e personit të autorizuar, stacionin e punës nga ku arrihet në sistemin e informacionit, datën dhe orën e qasjes, të dhënat personale te të cilat është arritur, llojin e qasjes me operacionet e ndërmarra gjatë përpunimit të të dhënave, dokument autorizimi për çdo hyrje, dokument për çdo hyrje të paautorizuar dhe dokument për largim automatik nga sistemi i informacionit.
(3) Во евиденцијата од ставот (1) на овој член се внесуваат и податоци за идентификување на информацискиот	(3) Në evidencën nga paragrafi (1) i këtij neni vendosen gjithashtu të dhënat për identifikimin e sistemit të informacionit

систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво на авторизација.	nga i cili është bërë përpjekje e jashtme për të hyrë në funksionet operative ose të dhënat personale pa nivelin e duhur të autorizimit.
(4) Операциите кои овозможуваат евидентирање на податоците од ставовите (2) и (3) на овој член треба да бидат контролирани од страна на офицерот за заштита на личните податоци и/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.	(4) Operacionet që mundësojnë evidentimin e të dhënave nga paragrafët (2) dhe (3) të këtij neni, duhet të kontrollohen nga zyrtari për mbrojtjen e të dhënave personale dhe/ose nga person tjetër i autorizuar nga kontrolluesi që ka njohuritë dhe aftësitë e nevojshme, por nuk ka privilegje administrative dhe të njëjtat detyrimisht duhet të rregullohen në atë mënyrë që të mos mund të çaktivizohen. Lidhur me evidencën e të dhënave për hyrje, kontrolluesi mund të përdorë gjithashtu vegla që të dhënat i gjenerojnë në formë të thjeshtë dhe të lehtë për lexim.
(5) Евиденцијата од ставот (1) на овој член се чува најмалку пет години.	(5) Evidenca nga paragrafi (1) i këtij neni mbahet të paktën pesë vjet.
(6) Офицерот за заштита на личните податоци врши контрола на податоците од ставовите (2) и (3) на овој член, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.	(6) Zyrtari për mbrojtjen e të dhënave personale kontrollon të dhënat nga paragrafët (2) dhe (3) të këtij neni, të paktën një herë në muaj përgatit raport për verifikimin e kryer dhe për parregullsitë e konstatuara.
(7) Контролорот ги известува овластените лица за воспоставениот систем за евиденција за пристап до информацискиот систем.	(7) Kontrolluesi i njofton personat e autorizuar për sistemin e vendosur për evidencë për qasje në sistemin e informacionit.
(8) 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.	(8) Kontrolluesi siguron mbrojtje të sistemit të evidencës për hyrje në sistemin e informacionit, nga çdo qasje e paautorizuar, veçanërisht për personat, veprimtaria e të cilëve evidentohet në sistemin e evidencave.

(9) 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.	9) Kontrolluesi siguron që personat e autorizuar për menaxhim me sistemin e evidentimit për të hyrë në sistemin e informacionit të njoftojnë kryesinë për çfarëdo anomalie ose incidenti të sigurisë, menjëherë, kurse më së voni në afat prej 12 orëve nga momenti i incidentit.
(10) 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.	(10) Kontrolluesi njofton Agjencinë për Mbrojtjen e të Dhënave Personale për çdo shkelje të sigurisë së të dhënave personale, e nëse ekziston probabiliteti të shkaktojë rrezik të lartë për të drejtat dhe liritë e personave fizikë dhe subjekteve të të dhënave personale, në mënyrë që t'i kufizojnë pasojat nga shkelja e sigurisë.
(11) 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).	(11) Kontrolluesi nuk guxon t'i përdorë informacionet nga evidenca për hyrje në sistemin e informacionit për ndonjë qëllim, ndryshe nga ajo që sistemi i informacionit është përdorur në mënyrë përkatëse (për shembull: përdorimi i regjistrave për matjen e orëve të punonjësit paraqet shpërdorim me sistemin e informacionit).
Обезбедување на преносливите медиуми	**Sigurimi i mediave portative**
Член 16	**Neni 16**
(1) 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.	(1) Kontrolluesi në bazë të analizës së rrezikut për shkeljen e sigurisë së të dhënave personale në rast të vjedhjes ose mënyrë tjetër të humbjes së mjeteve portative (pajisje mobile) në të cilat kryhet përpunimi i të dhënave personale, zbaton masa përkatëse teknike.
(2) Техничките мерките од ставот (1) на овој член го опфаќаат најмалку следното:	(2) Masat teknike nga paragrafi (1) i këtij neni përfshijnë së paku si në vijim:
подигање на свеста на овластените лица за	- ngritjen e vetëdijes së personave të autorizuar

специфичните ризици поврзани со користење на преносливи медиуми (на пример: кражба на опремата) и утврдените процедури за намалување на овие ризици;	për rreziqet specifike që lidhen me përdorimin e mediave portative (për shembull: vjedhjen e pajisjeve) dhe procedurat e përcaktuara për zvogëlimin e këtyre rreziqeve;
спроведување на мерки за правење на сигурносна резервна копија или синхронизација на мобилните работни станици, со цел да заштитат од губење на зачуваните податоци;	-zbatimin e masave për të bërë kopje rezervë të sigurisë ose sinkronizimin e stacioneve mobile të punës, me qëllim të mbrojtjes nga humbja e të dhënave të ruajtura;
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	- masat e kriptimit për mbrojtjen e stacioneve mobile të punës dhe mediave për deponim mobil (laptop, USB, hard disk të jashtëm, CD-ROM, DVD, etj) Për shembull: shumica e laptopëve përfshijnë funksionalitetin që mundëson të kriptohet hard disku i tyre, për çka çdoherë që është e mundshme rekomandohet të përdoret ky opsion); dhe
- употреба на услуги во облак (cloud services) за правење на сигурносни копии само по претходна анализа на нивните услови и безбедносни гаранции.	- përdorimi i shërbimeve në (cloud services) për të bërë kopje sigurie vetëm pas analizës paraprake të kushteve të tyre dhe garancive të sigurisë.
- (3) Покрај мерките од ставот (2) на овој член, врз основа на спроведената анализа на ризик, доколку се утврди за потребно, контролорот може да ги примени и следните мерки:	(3) Krahas masave nga paragrafi (2) i këtij neni, bazuar në bazë të analizës së kryer të rrezikut, nëse vërtetohet si e nevojshme, kontrolluesi mund t'i zbatojë edhe këto masa:
- 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;	-instalimin e një filtri privatësie në ekranet e stacioneve mobile të punës që përdoren në vende publike, ose përdorimin e stacioneve mobile të punës me një filtër të integruar të privatësisë;
- ограничување на обемот на податоци кои може да се зачуваат на мобилните	-kufizimi i vëllimit të të dhënave që mund të ruhen në stacionet mobile të punës në atë që

работни станици на она што е строго неопходно со дополнителна заштита и ограничување за време на патувања, особено во странство;	është rreptësisht e domosdoshme me mbrojtje dhe kufizime shtesë gjatë udhëtimit, sidomos jashtë vendit;
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	- zbatimi i masave shtesë për mbrojtje nga vjedhjet (për shembull kabllo sigurie, shenjimi i dukshëm i pajisjeve etj.) dhe masave që zvogëlojnë efektet negative (për shembull, mbyllje automatike, kriptim); dhe
- 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.	-kur pajisjet mobile përdoren për të mbledhur të dhëna në lëvizje (për shembull: asistentë personalë, telefona të mençur, laptopë etj.), shifrim të të dhënave të vetë pajisjes. Gjithashtu, mbyllje të pajisjes pas disa minutave mosfunksionim dhe pastrim të të dhënave të mbledhura pasi të transferohen në sistemin e informacionit të kontrolluesit.
Заштита на внатрешната мрежа	**Mbrojtja e rrjetit të brendshëm**
Член 17	**Neni 17**
(1) Контролорот обезбедува заштита на својата внатрешна мрежа преку овозможување само на неопходните мрежни функции потребни за обработка на личните податоци, а особено преку:	(1) Kontrolluesi siguron mbrojtje të rrjetit të tij të brendshëm duke mundësuar vetëm funksionet e nevojshme të rrjetit për përpunimin e të dhënave personale, sidomos nëpërmjet:
ограничување на пристапот до интернет со блокирање на несуштински услуги и сервиси (VoIP, peer to peer, итн.);	- kufizimit të qasjes në internet duke bllokuar shërbime jothelbësore (VoIP, peer to peer etj.);
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);	- menaxhimit të rrjetit Wi-Fi që përfshin përdorimin e metodave më moderne të kriptimit (për shembull: WPA2 ose WPA2-PSK dhe duke përdorur fjalëkalime komplekse që ndryshohen në kohë të përcaktuara);

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;	- rrjeti Wi-Fi që është i hapur për përdorimin e personave të paautorizuar (për shembull vizitorë të jashtëm) duhet të ndahet nga rrjeti i brendshëm;
- 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);	- në rast të hyrjes nga distanca, vendosje të domosdoshme të lidhjes VPN, me autentifikim të detyrueshëm të personit të autorizuar (për shembull: kartelë e mençur, pajisje për gjenerimin e fjalëkalimit një përdorim- OTP etj.);
- 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	- duke siguruar që asnjë panel administrues për udhëheqje me përmbajtje dhe cilësimet e sistemit të mos jetë në dispozicion direkt nëpërmjet internetit (mirëmbajtja në distancë doemos të kryhet nëpërmjet VPN); dhe
- ограничување на мрежниот сообраќај со филтрирање на влезниот/појдовниот сообраќај на опрема со заштитен ѕид, 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).	- kufizimit të trafikut të rrjetit duke filtruar trafikun hyrës/dalës të pajisjes me mur mbrojtës, serverë proksi etj. (për shembull: nëse serveri i internetit përdor HTTPS, të sigurohet që trafiku hyrës të jetë nëpërmjet portit 443 dhe duke bllokuar të gjitha qasjet e tjera).
- (2) Контролорот врз основа на анализата на ризикот, покрај мерките наведени во ставот (1) од овој член, може да примени и други мерки со кои ќе ја зајакне заштитата на својата внатрешна мрежа.	(2) Kontrolluesi në bazë të analizës së rrezikut, krahas masave nga paragrafi (1) i këtij neni, mund të zbatojë edhe masa të tjera me të cilat do ta forcojë mbrojtjen e rrjetit të tij të brendshëm.
Обезбедување на серверите	**Sigurimi i serverëve**

Член 18	Neni 18
(1) 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:	(1) Kontrolluesi, sipas analizës së rrezikut, është i obliguar që në krye të listës së tij, nga aspekti i zbatimit të masave teknike dhe organizative, t'i ketë serverët e tij, mbi të cilët centralizohet përpunimi i një sasie të madhe të të dhënave personale. Më pas, kontrolluesi zbaton në mënyrë të veçantë (të paktën) masat e mëposhtme:
единствено овластени лица кои ги имаат потребните знаења може да имаат пристап до алатките и административни панели на серверите;	- vetëm personat e autorizuar me njohuritë e nevojshme mund të kenë qasje në vegla dhe panelet administrative të serverëve;
примена на овластувања со помалку привилегии за лицата кои не се администратори на информацискиот систем (вообичаени операции за стандардни корисници);	- zbatimi i aftësive më pak privilegje për personat që nuk janë administratorë të sistemit të informacionit (operacione të zakonshme për përdorues standardë);
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...);	- zbatimi i një politike të veçantë për krijimin dhe përdorimin e fjalëkalimeve për administratorin e sistemit të informacionit (për shembull: ndryshimi i fjalëkalimeve pas çdo dalje të administratorit, përdorimi i fjalëkalimeve të shumëfishta...);
- 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);	- instalimi i të gjitha përditësimeve të rëndësishme (updates) për sistemet operative dhe aplikacionet në një interval kohor bazuar në analizën e rrezikut, por jo më gjatë se përditësim javor duke cilësuar sistemin e përditësimit automatik (auto update);
- правење на сигурносни копии и нивна редовна проверка; и	- bërja e kopjeve të sigurisë dhe kontrollimi i tyre i rregullt; dhe
- примена на TLS протокол (со замена	- zbatimi i protokollit TLS (me zëvendësimin e

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.	SSL13) ose protokollit tjetër që siguron kriptim dhe autenticitet, si minimum për çfarëdo shkëmbimi të të dhënave nëpërmjet Internetit dhe vërtetimi i zbatimit të tij përkatës nëpërmjet veglave përkatëse.
- (2) Во случај кога се врши администрирање на базите на податоци, контролорот ги применува најмалку следните мерки:	(2) Në rastet kur bëhet administrimi i bazave të të dhënave, kontrolluesi zbaton të paktën masat e mëposhtme:
- 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	- përdorimin e profileve të personalizuara për qasje në bazat e të dhënave dhe krijimin e një emri specifik përdoruesi për çdo aplikacion (specific account for each application); dhe
- примена на мерки против напади преку инјектирање на SQL код, скрипти и слично.	- zbatimin e masave kundër sulmit duke injektuar kodin SQL, skriptet dhe të ngjashme.
Обезбедување на веб-страницата на контролорот	**Sigurimi i faqes së internetit të kontrolluesit**
Член 19	**Neni 19**
(1) 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:	(1) Kontrolluesi që ka faqen e tij të internetit, duhet të zbatojë masa teknike me të cilat do të garantojë identitetin e saktë të faqes (pharming prevention), si dhe besueshmërinë e informacioneve që i dërgon ose mbledh nëpërmjet faqes së internetit, edhe atë sidomos nëpërmjet masave në vijim:
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	- implementimin e protokollit kriptografik (TLS zëvendësuar SSL) në të gjitha faqet e internetit të kontrolluesit (nëse ka më shumë se një), duke përdorur vetëm versionin e fundit dhe duke kontrolluar zbatimin e tij të duhur;

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;	- përdorimin e detyrueshëm të protokollit kriptografik (TLS) për të gjitha faqet e faqes së internetit, përfshirë formularët për mbledhjen e të dhënave personale ose mundësimin e vërtetimit të përdoruesit dhe të atyre ku shfaqen ose transmetohen të dhënat personale që nuk kanë qasje publike;
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;	- duke kufizuar portet e komunikimit të atyre që nevojiten rreptësisht për funksionimin e duhur të aplikacioneve të instaluara. Nëse ueb serveri pranon vetëm lidhje me HTTPS protokoll, lejohet vetëm trafik rrjeti IP që hyn nëpërmjet portit 443, dhe të gjitha portat e tjera të hyrjes duhet të bllokohen;
- 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	- duke siguruar që vetëm personat e autorizuar do të jenë në gjendje të përdorin mjete dhe interfejse administrative, ku të kufizohet përdorimi dhe të jetë e arritshme vetëm deri te personat e autorizuar me privilegje administratori të cilët janë pjesë e ekipit, përgjegjës për teknologjinë e informacionit dhe vetëm për aktivitete administrative që janë të domosdoshme; dhe
- 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;	- nëse përdoren biskotat që nuk janë të nevojshme nga shërbimi, kontrolluesi siguron pëlqim paraprak nga përdoruesi i Internetit pasi ta njoftojë përdoruesin, dhe para se të depozitohet biskota;
- (2) Контролорот кој има своја веб-страница не треба да применува практики кои го зголемуваат	(2) Kontrolluesi që ka faqen e tij personale nuk duhet të zbatojë praktika që rrisin rrezikun e abuzimit të mundshëm, përpunimit të padëshiruar (aksidental) ose të qëllimshëm të

ризикот од можна злоупотреба, несакана (случајна) или намерна неовластена обработка на личните податоци, а особено:	paautorizuar të të dhënave personale, dhe veçanërisht:
- да не пренесува лични податоци преку URL без примена на протокол за криптирање (на пример идентификатори или лозинки);	- të mos transmetojë të dhëna personale nëpërmjet URL-së pa zbatuar protokollin e kriptimit (për shembull identifikues ose fjalëkalime);
- користење на небезбедни услуги;	- shfrytëzim të shërbimeve të pasigurta;
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;	- përdorim të serverëve që hostojnë bazat të të dhënave ose serverë siç janë stacionet e punës, veçanërisht jo për kërkim në faqe interneti, qasje në mesazhe elektronike etj;
- поставување на базите на податоци на сервери кои се директно достапни преку интернет; и	- vendosje e bazave të të dhënave në serverë që janë drejtpërdrejt të arritshme nëpërmjet internetit; dhe
- споделување и употреба на корисничките сметки (user accounts) помеѓу две или повеќе овластени лица.	- ndarje dhe përdorim të llogarive të përdoruesve (user accounts) midis dy ose më shumë personave të autorizuar.
Обврски и одговорности на администраторот на информацискиот систем и на овластените лица	**Obligimet dhe përgjegjësitë e administratorit të sistemit të informacionit dhe të personave të autorizuar**
Член 20	**Neni 20**
(1) 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	(1) Kontrolluesi në bazë të analizës së zbatuar të rrezikut, përcakton obligimet dhe përgjegjësitë e administratorit të sistemit të informacionit dhe personave të autorizuar gjatë shfrytëzimit të dokumenteve dhe pajisjes së informacionit dhe komunikimit, duke zbatuar të paktën masat e parashikuara nga kjo Rregullore.

предвидени со овој правилник.	
(2) Контролорот задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.	(2) Kontrolluesi duhet të kryejë kontroll periodik mbi punën e administratorit të sistemit të informacionit dhe përgatit raport për kontrollin e kryer.
(3) Во извештајот од ставот (2) се наведуваат констатираните неправилности (доколку ги има) и предложените мерки за отстранување на тие неправилности.	(3) Raporti i përmendur në paragrafin (2) përmban parregullsi të konstatuara (nëse ka) dhe masat e propozuara për eliminimin e parregullsive.
(4) Контролорот задолжително ги информира администраторот и овластените лица од ставот (1) на овој член за документацијата за технички и организациски мерки која се однесува на извршувањето на нивните обврски и одговорности.	(4) Kontrolluesi detyrimisht informon administratorin dhe personat e autorizuar nga paragrafi (1) i këtij neni për dokumentacionin për masat teknike dhe organizative që ka të bëjë me kryerjen e obligimeve dhe përgjegjësive të tyre.
Превенирање, реакција и санирање на инциденти	**Parandalimi, reagimi dhe riparimi i incidenteve**
(обезбедување континуитет)	**(sigurimi i vazhdimësisë)**
Член 21	**Neni 21**
(1) 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.	(1) Kontrolluesi në bazë të analizës së rrezikut, vërteton planin e menaxhimin me vazhdimësinë e sistemit të informacionit, duke përfshirë listë të personave të autorizuar përgjegjës për parandalimin, si dhe për rivendosjen në kohë të qasjes në të dhënat personale dhe qasjen në to në rast të një incidenti fizik ose teknik.
(2) Согласно ставот (1) на овој член, контролорот го определува начинот на управување со инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци.	(2) Sipas paragrafit (1) të këtij neni, kontrolluesi përcakton mënyrën e menaxhimit me incidentet që cenojnë besueshmërinë, integritetin ose qasshmërinë e të dhënave personale.
(3) Управувањето со инциденти од ставот (2) на овој член, опфаќа пријавување, реакција и санирање на инцидентите, при што контролорот го определува начинот на	(3) Menaxhimi i incidenteve nga paragrafi (2) i këtij neni përfshin raportimin, reagimin dhe riparimin e incidenteve, ku kontrolluesi

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.	përcakton mënyrën e evidentimit të çdo incidenti, kohën e shfaqjes, personin e autorizuar që e ka paraqitur atë, për këtë janë paraqitur dhe masat e marra për riparimin e tij.
(4) Контролорот ги определува постапките кои се применуваат за повторно враќање на личните податоци и начинот на евидентирање на овластените лица од ставот (1) 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.	(4) Kontrolluesi përcakton procedurat e përdorura për marrjen e të dhënave personale dhe mënyrën e regjistrimit të personave të autorizuar nga paragrafi (1) i këtij neni, të cilët kanë kryer operacionet për marrjen e të dhënave personale, kategoritë e të dhënave personale të kthyera ose të cilat janë vendosur me dorë pas kthimit.
(5) Контролорот обезбедува дека овластените лица, обработувачите и подобработувачите знаат кого да го известат и предупредат во случај на настанат инцидент.	(5) Kontrolluesi siguron që personat e autorizuar, përpunuesit dhe nën-përpunuesit e dinë kë të njoftojnë dhe paralajmërojnë në rast të ndonjë incidenti.
(6) 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).	(6) Parandalimi i incidenteve përfshijnë të gjitha masat dhe kontrollet e vërtetuara me këtë Rregullore, dhe bazuar në analizën e realizuar të rrezikut (për shembull: përdorimi i energjisë së pandërprerë për ta mbrojtur pajisjen që përdoret për përpunimin e të dhënave personale, përdorimin e njëhershëm të shumta pajisjeve me radhë për ruajtjen e të dhënave personale /teknologjia RAID /, testimi i rregullt i funksionimit të pajisjes etj).
Сигурносни копии и повторно враќање на зачуваните лични податоци	**Kopjet e sigurisë dhe rikthimi i të dhënave personale të ruajtura**
(обезбедување континуитет)	**(sigurimi i vazhdimësisë)**
Член 22	**Neni 22**
(1) Контролорот врз основа на анализата на ризикот	(1) Kontrolluesi, bazuar në analizën e rrezikut,

прави сигурносни копии на личните податоци на редовни временски интервали, со цел да го намали ефектот во случај на нивно непосакувано губење или оштетување.	bën kopje të sigurisë së të dhënave personale në intervale të rregullta, me qëllim që të zvogëlojë efektin në rast të humbjes ose dëmtimit të tyre të padëshiruar.
(2) Сигурносните копии од ставот (1) на овој член 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).	(2) Kopjet e sigurisë nga paragrafi (1) i këtij neni duhet të bëhen dhe të testohen rregullisht, për të cilat kontrolluesi miraton Plan për sigurimin e vazhdimësisë (business continuity plan) që i parashikon të gjitha incidentet e mundshme (për shembull: incident në harduer).
(3) 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.	(3) Kontrolluesi, bazuar në analizën e rrezikut, vëllimin dhe dinamikën e kohës së ndryshimit të të dhënave, bën kopje të sigurisë në interval që minimizojnë rrezikun për efektin e të dhënave për të cilat në rast të ndonjë incidenti, do të ndodhte humbja ose dëmtimi i padëshiruar i tyre. Më pas, kontrolluesi bën një kopje të fragmentuar (incremental back-up) gjegjësisht kopje individuale në baza ditore në lidhje me të gjitha ndryshimet e bëra gjatë ditës, kurse kopje të plotë të sigurisë (full back-up) në intervalet të rregullta kohore pas vlerësimit të tij, të paktën një herë në muaj, në mënyrë ku do të garantojë rivendosjen e qasjes në të dhënat personale në rast të një incidenti fizik ose teknik.
(4) Контролорот задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личните податоци.	(4) Kontrolluesi doemos duhet të kontrollojë funksionalitetin e kopjeve të sigurisë për kryerjen e rindërtimit të të dhënave personale.
(5) Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат серверите и треба да се физички и криптографски заштитени, заради оневозможување на	(5) Kopjet e sigurisë ruhen jashtë hapësirës ku ndodhen serverët dhe duhet të jenë të mbrojtura fizikisht dhe në mënyrë kriptografike, për të pamundësuar çdo

каква било модификација.	modifikim.
(6) 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).	(6) Kontrolluesi në lidhje me kopjet e sigurisë duhet të përdorë të njëjtin nivel sigurie të masave teknike dhe organizative si për të dhënat e ruajtura në serverët operativë, mbi të cilët ai i përpunon të dhënat personale (për shembull: duke kriptuar kopjet e sigurisë, duke mbajtur në vend të sigurt kopjen e sigurisë për të cilën janë zbatuar masat dhe kontrollet që minimizojnë rrezikun e vërshimit, zjarrit, vjedhjeve etj, ose në rast të rregullimit kontraktues dhe autsorsimit të shërbimit, mbrojtja e duhur që duhet ta zbatojë përpunuesi).
Начин на архивирање и чување на податоците	**Mënyra e arkivimit dhe ruajtjes së të dhënave**
Член 23	**Neni 23**
(1) 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.	(1) Kontrolluesi, në lidhje me të dhënat personale për të cilat nuk ka skaduar afati i ruajtjes së tyre sipas ligjit, dhe për të cilin ka pushuar nevoja për përpunimin e tyre të drejtpërdrejtë dhe të përditshëm, kryen arkivimin në mënyrë të sigurt, përveç nëse të dhënat e arkivuara janë të dhëna të ndjeshme (kategori të posaçme të të dhënave personale), ose të dhëna që mund të kenë ndikim serioz ndaj subjekteve të të dhënave personale, nëse kompromethohen.
(2) Согласно ставот (1) од овој член, 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	(2) Sipas paragrafit (1) të këtij neni, kontrolluesi përcakton procedurë për menaxhimin e materialit arkivor lidhur me atë se cilat të dhëna duhet të arkivohen, si dhe ku ruhen dhe kush, si dhe me çfarë kushte ka qasje

и под кои услови има пристап до нив.	në to.
(3) 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.	(3) Kontrolluesi doemos miraton dokument të duhur “Lista (përmbledhja) me afate për ruajtjen e të dhënave personale”, i cili do të përmbajë informacione për momentin e aktivizimit të periudhës (afatin) për ruajtjen e të dhënave personale, periudhat e identifikuara (afatet) për ruajtjen e të dhënave personale, arsyet e ruajtjes së të dhënave personale, baza ligjore për ruajtjen e të dhënave personale dhe pronari i të dhënave.
(4) Контролорот е должен документот од ставот (3) на овој член да го ревидира и усогласува годишно согласно промените во работењето на контролорот и законските услови за чување на личните податоци.	(4) Kontrolluesi është i detyruar të rishikojë dhe harmonizojë dokumentin nga paragrafi (3) i këtij neni çdo vit në përputhje me ndryshimet në funksionimin e kontrolluesit dhe kushtet ligjore për ruajtjen e të dhënave personale.
Управување со преносливи медиуми	**Menaxhimi me mediat portative**
Член 24	**Neni 24**
(1) 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.	(1) Mediat portative në të cilat përpunohen të dhënat personale, kontrolluesi siguron që ato të mbahen në vend ku qasjen e kanë vetëm personat e autorizuar, të përcaktuar prej tij.
(2) Пренесувањето на медиумите од ставот (1) на овој член надвор од работните простории се врши само со претходно овластување од страна на контролорот.	(2) Transferimi i mediave nga paragrafi (1) i këtij neni jashtë hapësirave të punës kryhet vetëm me autorizim paraprak nga kontrolluesi.
(3) 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.	(3) Pas transferimit të të dhënave personale nga mediumi ose pas skadimit të periudhës së caktuar për ruajtje, mediumi duhet të shkatërrohet, fshihet ose pastrohen të dhënat personale të regjistruara në të.

(4) 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).	(4) Shkatërrimi i mediumit duhet të bëhet në atë mënyrë që do të garantojë se të dhënat e regjistruara në të nuk mund të rikonstruktohen përsëri (për shembull: me ndarje mekanike të pjesëve përbërësve të tij).
(5) Бришењето или чистењето на медиумот треба да се изврши на начин што ќе оневозможи понатамошно обновување на снимените лични податоци.	(5) Fshirja ose pastrimi i mediumit duhet të bëhet në atë mënyrë që të parandalojë ripërtëritjen e mëtejshëm të të dhënave personale të regjistruara.
(6) За случаите од ставовите (4) и (5) на овој член 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.	(6) Për çështjet nga paragrafët (4) dhe (5) të këtij neni, kontrolluesi duhet të sigurojë gjurmë informacioni (për shembull: procesverbal), i cili përmban të gjitha të dhënat për identifikimin e plotë të mediumit, si dhe për kategoritë e të dhënave personale të regjistruara në të njëjtin.
Криптирање на личните податоци	**Kriptimi i të dhënave personale**
Член 25	**Neni 25**
(1) 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.	(1) Kur kontrolluesi bazuar në analizën e rrezikut, dhe duke marrë parasysh natyrën, përmasën, kontekstin dhe objektivat e përpunimit të të dhënave personale, bën kriptimin e të dhënave personale, gjithmonë zbaton zgjidhjet më moderne të kriptimit teknik me të cilat siguron integritetin, besueshmërinë dhe autenticitetin e të dhënave personale.
(2) Во согласност со ставот (1) на овој член контролорот применува единствено признати и безбедни алгоритми за криптирање (како на пример: SHA-256, SHA-512 или SHA-341 како хаш функција, HMAC	(2) Sipas paragrafit (1) të këtij neni, kontrolluesi zbaton vetëm algoritmet e pranuara dhe të sigurta të kriptimit (siç janë: SHA-256, SHA-512 ose SHA-341 si funksion hash, HMAC duke përdorur SHA-256, bcrypt, scrypt ose PBKDF2

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.	për ruajtjen e fjalëkalimeve, AES ose AES-CBC për kriptim simetrik, RSA-OAEP v2.1 për kriptim asimetrik ...) kurse gjithashtu siguron mbrojtje të çelësave sekret të kriptimit me të drejta kufizuese të hyrjes dhe fjalëkalim të sigurt të krijuar posaçërisht për qasje.
(3) 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.	(3) Kontrolluesi do të miratojë procedurë të brendshme, ku detyrimisht rregullon menaxhimin e çelësave sekretë dhe certifikatave, duke marrë parasysh menaxhimin me rrezikun e fjalëkalimeve të harruara.
Физичка безбедност	**Siguria fizike**
Член 26	**Neni 26**
(1) 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:	(1) Kontrolluesi doemos duhet të zbatojë nivel të përforcuar të sigurisë në lidhje me hapësirat ku janë vendosur dhe ku ruhen serverët dhe pajisjet e rrjetit, nëpërmjet të cilave kryhet përpunimi i të dhënave personale duke zbatuar masat e duhura të cilat sigurojnë që vetëm personat e autorizuar posaçërisht nga kontrolluesi të kenë qasje, si dhe masa me të cilat zvogëlohet rreziku i kërcënimeve të mundshme, edhe atë:
инсталирање на алармни системи против упад и нивна периодична проверка;	- instalimin e sistemeve të alarmit kundër ndërhyrjeve dhe kontrollit periodik të tyre;
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;	- zbatimi i masave dhe kontrolleve për parandalimin e vjedhjeve, zjarreve, shpërthimeve, tymit, ujit, pluhurit, dridhjeve, ndikimeve kimike, pengesa në furnizimin me energji elektrike dhe rrezatimi elektromagnetik;

обезбедување безбедност на клучевите и шифрите за аларми кои овозможуваат пристап до просториите;	- sigurim të çelësave dhe kodeve të alarmit që mundësojnë hyrje në hapësira;
- 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);	- sigurim të fushave të ndara në objektin ku ruhen serverët sipas analizës së rrezikut (për shembull: përdorim të një kontrolli të veçantë për qasje në dhomën e serverëve);
- 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;	- listë e përditësuar e personave ose kategorive të personave të autorizuar për të hyrë në hapësirat ku ruhen pajisjet për përpunimin e të dhënave personale;
- 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;	- vendosjen e rregullave dhe metodave për kontrollimin e qasjes së vizitorëve, edhe atë të paktën të jenë të shoqëruar nga një person në kontrollues me vizitorët jashtë fushave për pranimin e palëve;
- посебна физичка заштита на ИТ-опремата преку специфични методи (систем за спречување на пожар, поплави, електрична енергија, климатизација, итн.);	- mbrojtje e veçantë fizike e pajisjeve së IT-së nëpërmjet metodave specifike (sistemi i parandalimit të zjarrit, përmbytjet, energjia elektrike, klimatizim etj.);
- одржување на просториите за серверите (климатизација, UPS, итн.).	- mirëmbajtja e dhomës së serverëve (klimatizim, UPS etj).
- водење на евиденција за пристап до просториите каде што се чуваат серверите кои содржат лични податоци;	- mbajtja e shënimeve për qasje në hapësirat ku ruhen serverët që përmbajnë të dhëna personale;
- 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	- duke siguruar që vetëm personat e autorizuar mund të hyjnë në hapësirat me qasje të kufizuar (për shembull: brenda hapësirave të kontrolluara për qasje, të gjithë personat të mbajnë identifikim të dukshëm (kartelë), si dhe rishqyrtim dhe përditësim të rregullt të lejeve

идентификација (картичка), како и преиспитување и редовно ажурирајте на дозволите за пристап до заштитените области).	të hyrjes në zonat e mbrojtura).
- (2) По исклучок од ставот (1) на овој член, серверите на кои се инсталирани софтверски програми за обработка на личните податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на контролорот.	(2) Me përjashtim nga paragrafi (1) të këtij neni, serverët në të cilët janë instaluar programe softuerike për përpunimin e të dhënave personale, mund të lokalizohen, hostohen dhe të administrohen jashtë hapësirave të kontrolluesit.
- (3) Во случајот од ставот (2) на овој член, 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.	(3) Në rastin e paragrafit (2) të këtij neni, të drejtat dhe detyrimet e ndërsjella të kontrolluesit dhe personit juridik, përkatësisht personit fizik, ku serverët janë të lokalizuar, të hostuar dhe të administruar fizikisht, duhet të rregullohen me marrëveshje me shkrim, e cila detyrimisht do të përmbajë masa për sigurinë e të dhënave personale, në përputhje me rregulloret për mbrojtjen e të dhënave personale.
Контрола на информацискиот систем и информатичката инфраструктура	**Kontrolli i sistemit të informacionit dhe infrastrukturës së informacionit**
Член 27	**Neni 27**
(1) Во документацијата за технички и организациски мерки утврдена во членот 10 од овој правилник, задолжително треба да се содржани постапките за овластување на офицерот за заштита на личните податоци, за вршење периодични контроли, заради следење на усогласеноста на работењето на контролорот со прописите за заштита на	(1) Në dokumentacionin për masat teknike dhe organizative të përcaktuara në nenin 10 të kësaj Rregullore, detyrimisht duhet të figurojnë procedurat e autorizimit të zyrtarit për mbrojtjen e të dhënave personale, për kryerjen e kontrolleve periodike, me qëllim të mbikëqyrjes të përshtatshmërisë së punës së kontrolluesit me dispozitat për mbrojtjen e të

личните податоци и со донесената документација за технички и организациски мерки.	dhënave personale dhe me dokumentacionin e miratuar për masat teknike dhe organizative.
(2) 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.	(2) Sistemi i informacionit të kontrollorit dhe infrastruktura e informacionit duhet t'i nënshtrohen kontrollit të brendshëm vjetor për të kontrolluar nëse procedurat dhe udhëzimet e përfshira në rregullat dhe politikat për sigurinë e të dhënave personale janë zbatuar dhe janë në përputhje me dispozitat për mbrojtjen e të dhënave personale.
Управување со обработувачи	**Menaxhimi me përpunuesit**
Член 28	**Neni 28**
(1) 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.	(1) Kontrolluesi është i obliguar të krijojë proces të menaxhimit kur përdor shërbime të përpunimit të të dhënave personale nga përpunuesit, me qëllim të vendosjes së procedurave të përshtatshme të vendimmarrjes në përzgjedhjen e përpunuesit, menaxhimin e përpunimit të të dhënave personale, si dhe përmbushjen e obligimeve të kontraktuara dhe përgjegjësive nga përpunuesi.
(2) Контролорот е должен да применува процедура за одлучување за избор на обработувач со која задолжително ќе предвиди:	(2) Kontrolluesi është i obliguar të zbatojë procedurë vendimmarrjeje për zgjedhjen e përpunuesit, me të cilin do të parashikojë detyrimisht:
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	1. Analiza e përpunuesve të mundshëm në lidhje me masat e tyre teknike dhe organizative për të siguruar që përpunimi i të dhënave personale do të bëhet në përputhje me kërkesat e parapara në dispozitat për mbrojtjen e të dhënave personale, si dhe për të siguruar mbrojtjen e të drejtave të subjekteve të të dhënave personale; dhe

2. Анализа на ризиците врз работењето на контролорот што можат да произлезат при обработката на личните податоци од страна на обработувачите.	2. Analiza e rrezikut për funksionimin e kontrolluesit që mund të paraqiten gjatë përpunimit të të dhënave personale nga përpunuesit.
Ангажирање на обработувачи	**Angazhimi i përpunuesve**
Член 29	**Neni 29**
(1) 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.	(1) Në rast se kontrolluesi vendos të transferojë gjëra nga sfera e tij e punës në lidhje me përpunimin e të dhënave personale të përpunuesit, ai është i obliguar të sigurojë që të dhënat personale përpunohen nën mbikëqyrjen e tij për sigurinë e të dhënave personale, ku të dhënat personale duhet të përpunohen me garanci të sigurisë.
(2) Во случаите од ставот (1) на овој член, 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.	(2) Në rastet e përmendura në paragrafin (1) të këtij neni, kontrollori mund të transferojë punime vetëm tek një procesor i cili mund të sigurojë garanci të mjaftueshme, veçanërisht në lidhje me njohuritë e nevojshme në fushën e mbrojtjes së të dhënave personale, sigurisë dhe burimeve.
(3) 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.	(3) Të drejtat dhe obligimet e ndërsjella të kontrolluesit dhe përpunuesit duhet të rregullohen me marrëveshje, ku kontrolluesi para lidhjes së kontratës obligohet të kërkojë nga përpunuesi (ofruesi i shërbimit) që të paraqesë politikën e tij të sigurisë në lidhje me sistemin e informacionit dhe infrastrukturën e informacionit në të cilën do të kryhet përpunimi i të dhënave personale në emër të kontrolluesit.
(4) Безбедносната политика од ставот (3) на овој член треба да содржи податоци со кои ќе се гарантита безбедноста на личните податоци, и тоа:	(4) Politika e sigurisë nga paragrafi (3) i këtij neni përmban të dhëna që garantojnë sigurinë e të dhënave personale, edhe atë:

дали и како се врши криптирање на податоците според нивната чувствителност;	- nëse dhe si bëhet kriptimi i të dhënave sipas ndjeshmërisë së tyre;
постоење на процедури кои гарантираат дека никој нема да има неовластен пристап до податоците;	- ekzistimi i procedurave që garantojnë se askush nuk do të ketë qasje të paautorizuar në të dhënat;
дали и како се врши криптирање на преносот на податоци;	- nëse dhe si bëhet kriptimi i të dhënave;
- гаранции во однос на следливост (логови, информациска ревизорска трага...);	- garanci për sa i përket vazhdueshmërisë (regjistra, gjurma e revidimit të informacionit...);
- управување со правата на пристап;	- menaxhimi i të drejtave të qasjes;
- автентикација; и	- autentifikimi; dhe
- други мерки за безбедност на обработката на личните податоци.	- masa të tjera për sigurinë e përpunimit të të dhënave personale.
- (5) Договорот од ставот (3) на овој член треба да содржи одредби особено за:	(5) Marrëveshja nga paragrafi (3) i këtij neni duhet të përmbajë dispozita sidomos për:
- предметот, должината и целта на обработката на личните податоци;	- lëndën, gjatësinë dhe qëllimin e përpunimit të të dhënave personale;
- обврските за обработувачот да преземе технички и организациски мерки за да обезбеди безбедност на обработката на личните податоци;	- obligimet që përpunuesi të marrë masa teknike dhe organizative për të siguruar sigurinë e përpunimit të të dhënave personale;
обврските во однос на доверливоста на доверените лични податоци;	- obligimet në lidhje me besueshmërinë e të dhënave personale të besuara;
- минималните стандарди за автентикација на овластените лица;	- standardet minimale për vërtetimin e personave të autorizuar;
- условите за враќање на податоците и/или нивно уништување по истекот или раскинувањето на договорот;	- kushtet për kthimin e të dhënave dhe/ose shkatërrimin e tyre pas skadimit ose zgjidhjes së kontratës;
- правилата за управување и известување на контролорот во случај на инциденти, односно во случај на нарушување на безбедноста на личните податоци;	- rregullat për menaxhimin dhe njoftimin e kontrolluesit në rast të incidenteve përkatësisht në rast të shkeljes së sigurisë së të dhënave personale;
- обврските за обработувачот да постапува единствено во согласност	- obligimet që përpunuesi të veprojë vetëm në përputhje me udhëzimet e marra nga

со упатствата добиени од страна на контролорот; и	kontrolluesi; dhe
- - другите обврски и одговорности согласно со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.	- obligimet dhe përgjegjësitë e tjera në përputhje me rregulloret për mbrojtjen e të dhënave personale dhe me dokumentacionin e miratuar për masat teknike dhe organizative.
2. Организациски мерки	**2. Masat organizative**
Организациски мерки за безбедност на личните податоци (минимален стандард)	**Masat organizative për sigurinë e të dhënave personale (standardi minimal)**
Член 30	**Neni 30**
(1) 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) Kontrolluesi është i obliguar të sigurojë masa të përshtatshme organizative për sigurinë e të dhënave personale bazuar në rezultatet e analizës së rrezikut të realizuar, e sidomos të sigurojë:
Ограничен пристап со идентификација за пристап до личните податоци;	Qasje të kufizuar duke identifikuar hyrjen në të dhënat personale;
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;	Rregulla organizative për qasjen e personave të autorizuar në internet që kanë të bëjnë me shkarkimin dhe incizimin e dokumenteve të marra nga posta elektronike dhe burime tjera;
Уништување на документи по истекот на рокот за нивно чување;	Shkatërrim të dokumenteve pas skadimit të periudhës për ruajtjen e tyre;
1. Мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци; и	1. Masa për sigurinë fizike të hapësirave të punës dhe pajisjeve të informacionit dhe komunikimit, ku mblidhen, përpunohen dhe ruhen të dhënat personale; dhe
2. Почитување на техничките упатства при инсталирање и користење на информатичко комуникациската опрема на која се обработуваат личните податоци.	2. Respektim të udhëzimeve teknike gjatë instalimit dhe përdorimit të pajisjes së informacionit dhe komunikimit në të cilat përpunohen të dhënat personale.

3. 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.	3. Personi i punësuar i cili kryen punën për burimet njerëzore te kontrolluesi, e informon administratorin e sistemit të informacionit për punësimin ose angazhimin e çdo personi të autorizuar me të drejtën e qasjes në sistemin e informacionit, në mënyrë që të caktohet një emër përdoruesi dhe fjalëkalimi, si dhe përfundimin e punësimit ose angazhimin që t'i fshihet emri i përdoruesit dhe fjalëkalimi përkatësisht të mbyllura për qasje të mëtejshme.
4. Известувањето од ставот (2) на овој член се врши и при било кои други промени во работниот статус или статусот на ангажирањето на овластеното лице што има влијание врз нивото на дозволениот пристап до информацискиот систем.	4. Njoftimi nga paragrafi (2) i këtij neni bëhet gjatë çfarëdo ndryshimi tjetër në statusin e punës ose statusin e angazhimit të personit të autorizuar që ka ndikim në nivelin e qasjes së lejuar deri në sistemin e informacionit.
Информирање и едуцирање за заштитата на личните податоци	**Informimi dhe edukimi për mbrojtjen e të dhënave personale**
Член 31	**Neni 31**
(1) 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.	(1) Personat që janë të punësuar ose janë të angazhuar me kontrolluesin, para fillimit të punës, njihen me rregulloren për mbrojtjen e të dhënave personale, si dhe me dokumentacionin e miratuar për masat teknike dhe organizative.

(2) 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.	(2) Për personat që janë të angazhuar për kryerjen e punës së kontrolluesit në kontratën për angazhimin e tyre, përcaktohen obligimet dhe përgjegjësitë për mbrojtjen e të dhënave personale.
(3) Контролорот пред непосредното започнување со работа на овластените лица, дополнително ги информира за непосредните обврски и одговорности за заштита на личните податоци.	(3) Kontrolluesi, para fillimit të drejtpërdrejtë të punës së personave të autorizuar, gjithashtu i informon ata rreth detyrave të drejtpërdrejta dhe përgjegjësive për mbrojtjen e të dhënave personale.
(4) 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.	(4) Personat që punësohen ose angazhohen te kontrolluesi, përpara se të fillojnë punën e tyre, nënshkruajnë deklaratë për fshehtësi dhe mbrojtje të përpunimit të të dhënave personale.
(5) Изјавата од ставот (4) на овој член особено содржи: дека лицата ќе ги почитуваат начелата за заштита на личните податоци пред нивниот пристап до личните податоци; ќе вршат обработка на личните податоци согласно упатствата добиени од контролорот, освен ако со закон поинаку не е уредено и ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита.	(5) Deklarata nga paragrafi (4) i këtij neni posaçërisht përmban: se personat do t'i respektojnë parimet e mbrojtjes së të dhënave personale para qasjes në të dhënat personale; do t'i përpunojnë të dhënat personale në përputhje me udhëzimet e marra nga kontrolluesi, po qe se nuk është e parashikuar me ligj dhe do t'i ruajnë të dhënat personale si të besueshme, si dhe masat për mbrojtjen e tyre.
(6) Изјавата од ставот (4) на овој член задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат кај контролорот.	(6) Deklarata nga paragrafi (4) i këtij neni duhet të mbahet në dosjet e personave që janë të punësuar ose të angazhuar te kontrolluesi.
(7) Контролорот задолжително врши континуирано информирање и едуцирање на раководството и овластените лица за непосредните обврски и одговорности за заштита на личните податоци.	(7) Kontrolluesi doemos kryen informim dhe edukim të vazhdueshëm të kryesisë dhe personave të autorizuar për obligimet dhe përgjegjësitë e drejtpërdrejta për mbrojtjen e të dhënave personale.
Пристап до документите	**Qasja në dokumente**
Член 32	**Neni 32**
(1) Пристапот до документите треба биде ограничен само за овластени лица на контролорот.	(1) Qasja në dokumente duhet të kufizohet vetëm për personat e autorizuar të kontrolluesit.

(2) 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.	(2) Për qasje në dokumente, doemos duhet të krijohen mekanizmat për identifikimin e personave të autorizuar dhe për kategoritë e të dhënave personale në të cilat ka qasje.
(3) 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.	(3) Nëse një person tjetër ka nevojë për qasje në dokumente, atëherë duhet të përcaktohen procedura të duhura për këtë qëllim në dokumentacionin për masat teknike dhe organizative.
Правило „чисто биро”	**Rregulli “zyra e pastër”**
Член 33	**Neni 33**
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.	Kontrolluesi duhet të zbatojë rregullin “zyra e pastër” gjatë përpunimit të të dhënave personale të përfshira në dokumente për mbrojtjen e tyre gjatë gjithë procesit të përpunimit nga qasja e personave të paautorizuar.
Чување на документи	**Ruajtja e dokumenteve**
Член 34	**Neni 34**
(1) Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отворање.	(1) Ruajtja e dokumenteve duhet të bëhet në atë mënyrë ku do të zbatohen mekanizma përkatës për pengimin e çdo hapjeje të paautorizuar.
(2) Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки кои што ќе го спречат секој неовластен пристап до документите.	(2) Kur karakteristikat fizike të dokumenteve nuk lejojnë zbatimin e masave nga paragrafi (1) i këtij neni, kontrolluesi duhet të zbatojë masa të tjera që parandalojnë çdo qasje të paautorizuar në dokumente.
(3) Ако документите не се чуваат заштитени на начин определен во ставовите (1) и (2) на овој член, тогаш контролорот треба да ги примени сите мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.	(3) Nëse dokumentet nuk mbahen të ruajtura në mënyrë të përcaktuar në paragrafët (1) dhe (2) të këtij neni, atëherë kontrolluesi duhet t’i zbatojë të gjitha masat për mbrojtjen e tyre gjatë gjithë procesit të përpunimit nga qasja e personave të paautorizuar.

Уништување на документи	**Shkatërrimi i dokumenteve**
Член 35	**Neni 35**
(1) Уништувањето на документите се врши со ситнење или со друг начин, при што истите повторно да не можат да бидат употребливи.	(1) Asgjësimi i dokumenteve bëhet me grimcim ose mënyrë tjetër, pas çka të njëjtat nuk mund të përdoren përsëri.
(2) Во случајот од ставот (1) на овој член комисиски се составува записник кој ги содржи сите податоци за целосна идентификација на документот како и за категориите на личните податоци содржани во истиот.	(2) Në rastin e paragrafit (1) të këtij neni, Komisioni përpilon procesverbal, i cili përmban të gjitha të dhënat për identifikimin e plotë të dokumentit, si dhe për kategoritë e të dhënave personale të përfshira në të.
Начин на чување на документите	**Mënyra e ruajtjes së dokumenteve**
Член 36	**Neni 36**
(1) 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.	(1) Dollapët, kartotekat ose pajisjet e tjera për ruajtjen e dokumenteve, doemos duhet të vendosen në hapësira të mbyllura me mekanizma të duhura mbrojtëse. Hapësirat gjithashtu duhet të mbyllen edhe për periudhën kur dokumentet nuk përpunohen nga personat e autorizuar.
(2) Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки за да се спречи секој неовластен пристап до документите.	(2) Kur karakteristikat fizike të hapësirave nuk lejojnë zbatimin e masave nga paragrafi (1) i këtij neni, kontrolluesi duhet të zbatojë masa tjera për të parandaluar çdo qasje të paautorizuar në dokumente.
IV. ВИСОКО НИВО	**IV. NIVELI I LARTË**
1. Технички мерки	**1. Masat teknike**
Дополнителни мерки	**Masat shtesë**

Член 37	Neni 37
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.	Bazuar në analizën e rrezikut, kontrolluesi prezanton dhe zbaton masa shtesë për sigurinë e të dhënave personale, me të cilat do të demonstrojë përputhshmëri shtesë me dispozitat dhe praktikat e mira për mbrojtjen e të dhënave personale.
Управување со лозинки	**Menaxhimi me fjalëkalimet**
Член 38	**Neni 38**
(1) 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.	(1) Kontrolluesi duhet të përdorë mjete për menaxhimin e fjalëkalimeve që sigurojnë se fjalëkalime të ndryshme për secilin shërbim ose program softuerik janë ruajtur në mënyrë përkatëse, ku për qasje në të gjitha fjalëkalimet siguron një fjalëkalim kryesor (master password), që duhet të përforcohet në mënyrë komplekse përkatësisht të përbëhet nga kombinimi i të paktën 12 karaktereve alfanumerike (shkronja/shkronja të vogla dhe të mëdha/), simbole, numra dhe shenja të veçanta pikësimi) dhe të ndryshohet në një periudhë jo më shumë se 30 ditë.
(2) 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).	(2) Kontrolluesi sipas analizës së rrezikut, për persona të caktuar të autorizuar (për shembull për administratorin e sistemit të informacionit ose personat që krijojnë dhe përdorin fjalëkalimin kryesor (master password), mund të shpërndajë rrezikun duke menaxhuar fjalëkalimin me faktor shtesë sipas rregullit n-2 (për shembull: informacioni për fjalëkalimin të ndahet në dy ose më shumë njerëz që do të regjistrohen së bashku, në atë mënyrë që secili do të dijë vetëm një pjesë të informacionit që e përbën fjalëkalimin, ose një person i autorizuar e di fjalëkalimin, kurse një tjetër e posedon dhe përdor kartë të mençur- smart card).

Сертификација за заштита на личните податоци	**Certifikim për mbrojtjen e të dhënave personale**
Член 39	**Neni 39**
Контролорот, покрај внатрешната контрола од член 27 на овој правилник, 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.	Kontrolluesi, përveç kontrollit të brendshëm nga neni 27 i kësaj Rregullore, në bazë vullnetare, mund të kontrollojë proceset dhe dokumentet e brendshme për mbrojtjen e të dhënave personale, për shkak të certifikimit të proceseve, nëpërmjet të cilave përpunohen të dhënat personale, në mënyrë që të demonstrojnë pajtueshmërinë me dispozitat për mbrojtjen e të dhënave personale gjatë operacioneve të përpunimit. Certifikimi kryhet nga Agjencia ose nga organet certifikuese në përputhje me dispozitat për mbrojtjen e të dhënave personale.
Управување со преносливи медиуми	**Menaxhimi me mediat portative**
Член 40	**Neni 40**
(1) 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.	(1) Kontrolluesi është i obliguar të krijojë sistem për evidentimin e mediave të pranuara në mënyrë që të mundësojë identifikimin e drejtpërdrejtë ose indirekt të llojit të medias së pranuar, datën dhe kohën e pranimit, dërguesit, numrin e mediave të pranuara, llojin e dokumentit i cili është regjistruar në medium, mënyra e dërgimit të mediumit, emrit dhe mbiemrit të personit të autorizuar për pranim të mediumit.
(2) Одредбите од ставот (1) на овој член се применуваат и за евидентирање на медиумите кои се испраќаат од страна на контролорот.	(2) Dispozitat e paragrafit (1) të këtij neni zbatohen edhe për evidentimin e mediave të dërguara nga kontrolluesi.
(3) 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.	(3) Për mediat e transmetuara jashtë hapësirave të punës së kontrolluesit, duhet të merren masat e nevojshme për ta parandaluar përpunimin e paautorizuar të të dhënave personale të regjistruara në to.
Тестирање на информацискиот систем	**Testimi i sistemit të informacionit**
Член 41	**Neni 41**
(1) Контролорот задолжително врши тестирање на информацискиот систем пред неговото имплементирање или по извршените промени со цел да се провери дали системот обезбедува	(1) Kontrolluesi doemos teston informacionin para zbatimit të tij ose pas ndryshimeve të kryera, që të shihet nëse sistemi siguron sigurinë e të dhënave personale në përputhje me dispozitat për mbrojtjen e

безбедност на личните податоци согласно со прописите за заштита на личните податоци.	të dhënave personale.
(2) Тестирањето од став (1) на овој член се врши преку обработка на документи кои содржат имагинарни лични податоци.	(2) Testimi nga paragrafi (1) i këtij neni kryhet nëpërmjet përpunimit të dokumenteve që përmbajnë të dhëna personale imagjinare.
Сертификациони постапки	**Procedurat certifikuese**
Член 42	**Neni 42**
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.	Kontrolluesi mund të zbatojë masa të tjera teknike për fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale, duke zbatuar procedurat e certifikimit në dispozitat që rregullojnë përdorimin e dokumenteve elektronike, identifikimin elektronik dhe shërbimet e besueshme.
Пренесување на медиуми	**Transferimi i mediave**
Член 43	**Neni 43**
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.	Mediat mund të transferohen nga hapësirat e punës vetëm nëse të dhënat personale janë të kriptuara ose të mbrojtura me metoda të përshtatshme që garantojnë se të dhënat nuk do të jenë të lexueshme, ku vetëm administratori i sistemit të informacionit mund t'i deshifrojë ose person i autorizuar nga ai.
Пренесување на личните податоци преку мрежа за електронски комуникации	**Transferimi i të dhënave personale nëpërmjet rrjetit të komunikimeve elektronike**
Член 44	**Neni 44**
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.	Të dhënat personale mund të transmetohen vetëm në rrjetin e komunikimeve elektronike nëse ato janë të kriptuara ose nëse janë të mbrojtura me metoda të përshtatshme që garantojnë se të dhënat nuk do të jenë të lexueshme gjatë transmetimit.
2. Организациски мерки	**2. Masat organizative**
Копирање и умножување на документите	**Kopjimi dhe shumimi i dokumenteve**

Член 45	Neni 45
(1) 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.	(1) Kopjimi ose shumimi i dokumenteve mund të bëhet vetëm nga persona të autorizuar, të përcaktuar me procedurë nga kontrolluesi ku doemos përcaktohen masat dhe mënyra e kopjimit dhe shumimit të dokumenteve.
(2) Уништувањето на копиите или умножените документи треба да се изврши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.	(2) Shkatërrimi i kopjeve ose dokumenteve të shumëzuara duhet të bëhet në atë mënyrë që të parandalojë përsëritjen e mëtejshme të të dhënave personale të përmbajtura.
Пренесување на документи	**Transferimi i dokumenteve**
Член 46	**Neni 46**
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.	Në rast të transferimit fizik të dokumenteve, kontrolluesi duhet të marrë masa për mbrojtjen e tyre nga qasja e paautorizuar ose trajtimi i të dhënave personale të përfshira në dokumentet e transferuara.
V. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ	**V. DISPOZITA KALIMTARE DHE PËRFUNDIMTARE**
Период на прилагодување	**Periudha e përshtatshmërisë**
Член 47	**Neni 47**
Во смисла на член 119 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија” бр. 42/20), контролорите и обработувачите се должни да го прилагодат своето работење со одредбите на овој правилник во рамките на периодот предвиден за усогласување со одредбите од Законот за заштита на личните податоци.	Në kuptim të nenit 119 të Ligjit për Mbrojtjen e Të dhënave Personale (“Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr. (42/20), kontrolluesit dhe përpunuesit obligohen ta përshtatin punën e tyre me dispozitat e kësaj Rregullore brenda periudhës së parashikuar për përshtatje me dispozitat e Ligjit për Mbrojtjen e Të Dhënave Personale.
Престанување на важење	**Ndërprerja e vlefshmërisë**
Член 48	**Neni 48**

Со денот на влегувањето во сила на овој правилник престанува да важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија” бр. 98/03 и 158/10) освен за случаите предвидени во членот 117 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија” бр. 42/20).	Me hyrjen në fuqi të kësaj Rregullore, ndërpritet vlefshmëria e Rregullores për masat teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjen e përpunimit të të dhënave personale (Gazeta Zyrtare e Republikës së Maqedonisë nr. 98/03 dhe 158/10) përveç rastet e parashikuara në nenin 117 të Ligjit për Mbrojtjen e Të Dhënave Personale (“Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr. 42/20).
Влегување во сила	**Hyrja në fuqi**
Член 49	**Neni 49**
Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија”.	Kjo Rregullore hyn në fuqi në ditën e tetë nga dita e botimit në “Gazetën Zyrtare të Republikës së Maqedonisë së Veriut”.
Бр. ____-_____/____	**Директор,** **Imer Aliu** Nr. ____-_____ / ____
_____._____.2020	_____._____.2020