Народна банка на Република Северна Македонија

ПОЛИТИКА
за сигурност на информацискиот систем

јуни 2021 година

Врз основа на член 47 став 1 точка 9 од Законот за Народната банка на Република Северна Македонија („Службен весник на Република Македонија" бр. 158/10, 123/12, 43/14, 153/15, 6/16 и 83/18 и „Службен весник на Република Северна Македонија" бр. 110/21 и 74/24), Советот на Народната банка на Република Северна Македонија донесе

ПОЛИТИКА
за сигурност на информацискиот систем
(неофицијален пречистен текст)[1]

I. ОПШТИ ОДРЕДБИ

1. Со Политиката за сигурност на информацискиот систем (во понатамошниот текст: ПСИС) се утврдува начинот на обезбедување сигурност на информациите и информацискиte средства, преку превентивно спроведување контроли за намалување на негативните ефекти предизвикани од појава на настани што ја загрозуваат сигурноста на информацискиот систем на Народната банка на Република Северна Македонија (во понатамошниот текст: Народната банка).

2. Целта на ПСИС е да обезбеди:
   - **доверливост** – информациите и информацискиte средства да бидат заштитени од неовластен пристап и достапни единствено на лица кои имаат овластување за пристап;
   - **интегритет** – информациите и информацискиte средства да бидат точни, целосни и ажурни; и
   - **достапност** – овластените корисници да имаат непречен пристап и постојана расположливост на информациите и информацискиte средства кога ќе имаат деловна потреба за тоа.

3. Настан што ја загрозува сигурноста на информацискиот систем е оној настан што предизвикува или може да предизвика нарушување на доверливоста, интегритетот и достапноста на информациите и информацискиte средства.

4. Информациите и информацискиte средства претставуваат витален сегмент во функционирањето на Народната банка и се користат единствено за службени потреби. Вработените, именуваните лица и други лица работно ангажирани во Народната банка имаат обврска соодветно да ги заштитуваат информациите и информацискиte средства согласно со оваа политика и со интерните акти.

5. ПСИС ќе се развива и ќе се усогласува со меѓународните стандарди за управување со сигурноста на информацискиte системи.

II. ОБЕЗБЕДУВАЊЕ НА СИГУРНОСТА НА ИНФОРМАЦИСКИОТ СИСТЕМ НА НАРОДНАТА БАНКА

[1] Ова претставува неофицијален пречистен текст на Политиката за сигурност на информацискиот систем. Истиот е составен од Политиката за сигурност на информацискиот систем П. бр. 02-15/IX-1/2021 од 30 јуни 2021 година и Политиката за изменување и дополнување на Политиката за сигурност на информацискиот систем Бр. 02-27277/6 од 25 јули 2024 година.

6. Советот на Народната банка се информира за состојбите во однос на спроведувањето на сигурносните стандарди и сигурноста на информацискиот систем еднаш годишно.

7. Гувернерот на Народната банка обезбедува интегрирање на контролите за сигурност на информацискиот систем во системот на интерни контроли на Народната банка преку:
   - обезбедување поддршка на процесот на информациска сигурност;
   - воспоставување централизиран надзор и координација;
   - дефинирање на соодветните улоги и одговорности;
   - следење на степенот на усогласеност на работењето на Народната банка со ПСИС.

8. Гувернерот на Народната банка формира Надзорен одбор за информацискиот систем на Народната банка заради набљудување на активностите за спроведување на ПСИС, како и за следење на останатите технолошки промени и надградби што ќе се вршат на информацискиот систем на Народната банка.

9. Надзорниот одбор за информацискиот систем го известува гувернерот на Народната банка за своето работење. Начинот на работа на Надзорниот одбор за информацискиот систем се уредува со деловник за работа.

10. Главното и помошник главното одговорно лице за сигурност на информацискиот систем, заштита на личните податоци и класифицирани информации од Канцеларијата за стратегија и превенција се лица *одговорни за сигурноста на информацискиот систем (во понатамошниот текст: ОСИС).* ОСИС има целосна самостојност и независност во своето работење и за својата работа му одговара на гувернерот на Народната банка.

11. ОСИС е одговорно за предлагање и следење на спроведувањето на ПСИС и на сите интерни акти коишто ќе произлезат од ПСИС. ОСИС врши надзор на почитувањето на одредбите на ПСИС и е должно да предлага ажурирање на ПСИС при настанати промени коишто ја загрозуваат сигурноста на информацискиот систем, како и при измени во организациската поставеност и технолошка платформа на Народната банка.

12. ОСИС ги има следниве права и надлежности:
   - врши координација на сите сигурносни активности во однос на информацискиот систем на Народната банка;
   - врши анализа и проценка на ризиците во однос на сигурноста на информацискиот систем;
   - дава предлози за спроведување и развој на ПСИС;
   - предлага интерни акти до гувернерот со кои се обезбедува посигурен информациски систем;
   - соработува со Дирекцијата за внатрешна ревизија околу предметот на годишната ревизија за сигурноста на информацискиот систем;
   - врши централна координација и истрага на настаните што ја загрозиле сигурноста на информацискиот систем, вклучувајќи и соработка со надворешни институции;
   - соработува со организациската единица задолжена за физичка сигурност, заштита и спасување на вработените и материјалните добра;
   - соработува со Дирекцијата за правни работи при изработката на интерните акти од областа на сигурноста на информацискиот систем, како и одредбите

коишто треба да се уредат во договорите со трети лица во врска со заштитата на личните податоци, класифицираните информации и други информации со одреден степен на тајност до кои ќе имаат пристап третите лица во текот на спроведувањето на договорот;
- организира обука на вработените за спроведување на ПСИС;
- има пристап до сите контролни дневници на ниво на информацискиот систем на Народната банка и
- им обезбедува советодавни услуги на лицата кои имаат пристап до информацискиот систем на Народната банка заради правилно спроведување на ПСИС и на соодветните интерни акти.

13. На предлог на гувернерот на Народната банка, Советот на Народната банка со овластување определува овластено лице *за заштита на личните податоци (во понатамошниот текст: ОЗЛП)*, на период од 4 години. ОЗЛП има целосна самостојност и независност во своето работење.

14. ОЗЛП директно одговара пред Советот на Народната банка којшто обезбедува дека тој:
    - на соодветен начин и навремено е вклучен во сите прашања поврзани со заштитата на личните податоци,
    - има ресурси неопходни за извршување на задачите,
    - има пристап до личните податоци и операциите на обработка,
    - непречено го одржува неговото стручно знаење,
    - не добива никакви упатства од највисокото раководно ниво во однос на извршувањето на неговите задачи и не може да биде сменет или казнет за извршувањето на своите задачи,
    - не извршува други задачи и должности коишто можат да доведат до судир на интереси.

15. ОЗЛП ги има следниве права и надлежности:
    - ги изработува интерните акти за заштита на личните податоци и ја следи нивната усогласеност со законот и со подзаконските акти за заштита на личните податоци;
    - ги информира, предлага обуки, дава мислења, совети и препораки, работи на подигнување на свеста и обучување на раководството и вработените кои вршат обработка на личните податоци за нивните обврски во однос на одредбите од Законот за заштита на личните податоци (во натамошниот текст: ЗЛП);
    - ја следи усогласеноста со ЗЛП, со други закони коишто се однесуваат на заштитата на личните податоци, усогласеноста на интерните акти на Народната банка во однос на заштитата на личните податоци, вклучувајќи распределување на одговорности;
    - спроведува ревизии/контроли за заштита на личните податоци и доставува годишен извештај за усогласеноста на Народната банка со прописите за заштита на личните податоци до Советот на Народната банка;
    - кога е потребно, дава совети во однос на проценатa на влијанието на заштитата на личните податоци и го следи извршувањето на проценатa во согласност со ЗЛП;
    - соработува со Агенцијата за заштита на лични податоци и дејствува како точка за контакт со неа во однос на прашања поврзани со обработката на личните податоци, вклучувајќи ја претходната консултација со Агенцијата пред обработката, ако проценатa на влијанието на заштитата на личните податоци покаже дека, доколку не се преземат мерки за ублажување на

ризикот, тогаш обработката на личните податоци ќе предизвика висок ризик за правата и слободите на физичките лица;
- дејствува како точка за контакт со субјектите на личните податоци за сите прашања поврзани со обработката на нивните лични податоци и за остварувањето на нивните права според ЗЛП;
- врши анализа на извештаите од супервизијата спроведена од страна на Агенцијата за заштита на личните податоци и доставува до гувернерот предлози за преземање потребни мерки за отстранување на утврдените недостатоци;
- врши проверка на евидентираните настани во системот за управување со ревизорските траги и
- може да врши и други задачи и должности доколку тие не доведуваат до судир на интереси.

16. Освен обврските од точките 12 и 15, ОСИС и ОЗЛП се должни да ја почитуваат доверливоста на документите, податоците и информациите до кои ќе пристапат во текот на извршувањето на своите работни задачи.

17. Тактичките раководители се одговорни за:
- подготовка и ажурирање на интерните процедури за работа во согласност со ПСИС;
- анализа и проценка на ризиците во однос на сигурноста на информацискиот систем во рамките на организациските единици со кои раководат и,
- проценка на влијанието на заштитата на личните податоци, доколку раководат со организациска единица што врши обработка на личните податоци.

18. Вработените во Народната банка се должни да ги почитуваат ПСИС и соодветните интерни акти за обезбедување сигурност на информацискиот систем.

19. Вработените во Народната банка се должни да ги известат тактичките раководители и ОСИС/ОЗЛП во случај кога:
- ќе утврдат дека се случил настан што ја загрозил сигурноста на информацискиот систем;
- ќе утврдат пречки во работењето на информацискиот систем; и
- се сомневаат дека е можно случување на настан што ја загрозува сигурноста на информацискиот систем.

20. Вработените во Народната банка се должни да применуваат соодветни мерки во случаи кога надворешни субјекти имаат пристап до делови од информацискиот систем на Народната банка, во согласност со ПСИС и соодветните интерни акти.

21. Дирекцијата за внатрешна ревизија (во натамошниот текст: ДВР) врши ревизија на адекватноста и ефективноста на системот на интерни контроли за сигурност на информацискиот систем во Народната банка и проверува дали се применуваат постапките и упатствата содржани во документацијата за техничките и организациските мерки за безбедност на личните податоци и дали тие се во согласност со прописите за заштита на личните податоци.

21-а. ДВР ги планира ревизиите врз основа на спроведена анализа на ризикот и расположливите ресурси на ДВР, земајќи ги предвид операциите, обемот и начинот на обработка на личните податоци, а во согласност со Годишната програма за работа на ДВР донесена од Советот на Народната банка.

21-б. ДВР изготвува извештаи за ревизиите од точката 21 во согласност со Политиката за внатрешна ревизија. ДВР изготвува годишен извештај за делот којшто се однесува на безбедноста на личните податоци и го доставува до гувернерот и до офицерот за заштита на личните податоци.

Начела поврзани со обработката на личните податоци

22. Народната банка применува соодветни технички и организациски мерки за обезбедување на обработката на личните податоци во согласност со закон, при што ги применува следниве начела:

- законитост, правичност и транспарентност – обработката се врши согласно со закон, во доволна мера и на транспарентен начин во однос на субјектот на личните податоци;
- ограничување на целите – податоците се собираат за конкретни, јасни и легитимни цели и не се обработуваат на начин што не е во согласност со тие цели;
- минимален обем на податоци – податоците што се обработуваат се соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради коишто се обработуваат;
- точност – податоците се точни и каде што е потребно ажурирани, при што се преземаат соодветни мерки за навремено бришење или коригирање на податоците што се неточни или нецелосни, имајќи ги предвид целите заради кои биле обработени;
- ограничување на рокот на чување – податоците се чуваат во форма којашто овозможува идентификација на субјектите на личните податоци, не подолго од она што е потребно за остварување на целите поради кои се обработуваат; и
- интегритет и доверливост – податоците се обработуваат на начин којшто обезбедува соодветно ниво на безбедност, вклучувајќи заштита од неовластена или незаконска обработка, како и нивно случајно губење, уништување или оштетување.

III. ЗАВРШНИ ОДРЕДБИ

23. Гувернерот на Народната банка донесува интерни акти со кои се спроведува ПСИС.

24. Со стапувањето во сила на оваа политика, престанува да важи Политиката за сигурност на информацискиот систем на Народната банка П. бр. 02-15/IX-5/2011 од 15.9.2011 година, П. бр. 02-15/I-2/2015 од 29 јануари 2015 година и П. бр.02-15/III-2/2016 од 24 март 2016 година.

25. Оваа политика за сигурност на информацискиот систем влегува во сила на денот на донесувањето.

Гувернер
и претседавач
на Советот на Народната банка
на Република Северна Македонија
д-р Анита Ангеловска-Бежоска

Скопје