



2026-01-2332

Na podlagi prvega odstavka 31. člena in tretjega odstavka 47. člena Zakona o Banki Slovenije (Uradni list RS št. 72/06 – uradno prečiščeno besedilo, 59/11, 55/17 in 15/26 – ZBan-4) Svet Banke Slovenije izdaja

Sklep o varovanju zaupnih informacij Banke Slovenije

I. POGLAVJE SPLOŠNO

1. člen (namen in obseg)

(1) Ta sklep opredeljuje:

- merila za določanje zaupnih informacij Banke Slovenije ter
- postopke ravnanja z zaupnimi informacijami Banke Slovenije, vključno z ukrepi za zaščito zaupnosti informacij Banke Slovenije.

(2) Ta sklep morajo za zakonito in pravno dopustno upravljanje zaupnih informacij Banke Slovenije uporabljati vsi zunanji in notranji prejemniki teh informacij.

(3) Vsak, ki razpolaga ali obdeluje zaupne informacije Banke Slovenije, je odgovoren za njihovo varovanje in ohranitev njihove zaupnosti skladno s predpisi in zahtevami, ki so določene s tem sklepom oziroma drugimi dogovori in ureditvami, ki veljajo med Banko Slovenije in posameznim prejemnikom.

(4) Ta sklep se ne uporablja za informacije, ki se štejejo za tajne podatke v skladu z zakonom, ki ureja tajne podatke.

2. člen (pomen izrazov)

Izrazi, uporabljeni v tem sklepu, pomenijo:

- »informacija Banke Slovenije« je vsakršna informacija ali podatek, ki jih Banka Slovenije pridobi, izdelava, shranjuje ali na kakršenkoli način obdeluje med izvajanjem svojih pristojnosti ter opravljanjem svojih nalog,
- »dokument« je izvirni ali reproducirani (pisan, risan, fotografiran) zapis v fizični, elektronski (digitalni), magnetni, optični ali drugi obliki, ki vsebuje informacije Banke Slovenije,
- »obdelava informacij« pomeni zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporabo, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje. Obdelava je lahko ročna ali avtomatizirana,
- »zunanji prejemnik« je pravna ali fizična oseba, ki na zakoniti podlagi od Banke Slovenije pridobi in obdeluje zaupne informacije Banke Slovenije,
- »iznos informacije iz sistema« pomeni tiskanje, shranjevanje na elektronski nosilec podatkov

(USB-ključ, CD/DVD-nosilec podatkov, zunanji disk in drugi) ali izmenjavo z drugim sistemom prek medsebojne povezave sistemov,

– »nosilec podatka« je vsak medij, na katerem so zapisani podatki v fizični obliki (npr. dokumenti v papirni obliki, fotografije in druge tiskovine) ali elektronski obliki (npr. trdi disk, CD/DVD, USB ipd).

II. POGLAVJE DOLOČANJE IN TRAJANJE ZAUPNOSTI

3. člen (stopnje zaupnosti)

(1) Informacije v Banki Slovenije se razvrščajo v eno od naslednjih stopenj zaupnosti:

- BSI-JAVNO,
- BSI-NEJAVNO,
- BSI-OMEJENO,
- BSI-ZAUPNO in
- BSI-TAJNO.

(2) Stopnja zaupnosti določene informacije Banke Slovenije se določi glede na oceno negativnega vpliva v primeru neupravičenega ali nepooblaščenega razkritja ali obdelave te informacije. Kriteriji za oceno negativnega vpliva za določanje stopnje zaupnosti informacije so določeni v prilogi 1 tega sklepa.

4. člen (zaupne informacije)

(1) Zaupna informacija Banke Slovenije po tem sklepu je vsaka informacija, ki jo ustvari Banka Slovenije in ki jo Banka Slovenije skladno s tem sklepom označi kot »BSI-NEJAVNO«, »BSI-OMEJENO«, »BSI-ZAUPNO« ali »BSI-TAJNO«, ali informacija, ki se glede na oceno negativnega vpliva, kot sledi iz kriterijev v prilogi 1, razumno šteje kot zaupna informacija Banke Slovenije z določeno stopnjo zaupnosti.

(2) Z oznakami iz prejšnjega odstavka se označujejo tudi dokumenti z informacijami, ki predstavljajo poslovno skrivnost.

(3) Informacija, ki je bila določena kot zaupna informacija zato, da bi se prikrilo storjeno kaznivo dejanje, prekršček ali zloraba pooblastil ali prikrilo kakšno drugo nezakonito dejanje ali ravnanje, se ne šteje kot zaupna informacija Banke Slovenije.

(4) Informacije, ki so na podlagi zakona javne, se ne smejo določiti kot zaupne informacije Banke Slovenije.

5. člen (varovanje zaupnih informacij)

Zaposleni in druge osebe, ki opravljajo delo za Banko Slovenije, so dolžni v okviru svojih delovnih nalog na podlagi kriterijev določenih s tem sklepom presoјati zaupnost posamezne informacije ob njenem nastanku, ob prejemu, ali ob začetku izvajanja naloge, katere rezultat bo zaupna informacija, ter glede na zaupnost informacije upoštevati ukrepe za njeno varovanje v skladu s tem sklepom.

6. člen
(pooblašćene osebe za določanje stopnje zaupnosti na dokumentih in drugih nosilcih podatkov)

(1) Stopnjo zaupnosti dokumenta oziroma drugega nosilca podatkov, ki vsebuje zaupne informacije Banke Slovenije, ob pogojih in na način, doloćen s tem sklepom, določi pooblašćena oseba Banke Slovenije. Dokumentu, ki vsebuje informacije Banke Slovenije različnih stopenj zaupnosti, se določi stopnja zaupnosti, ki ustreza najvišji stopnji zaupnosti informacij, ki so vključene v dokument. Nosilcu podatkov se določi stopnja zaupnosti, ki ustreza najvišji stopnji zaupnosti dokumentov, ki so shranjeni na nosilcu podatkov.

(2) Pooblašćene osebe Banke Slovenije so:

- a) člani Sveta Banke Slovenije,
- b) generalni sekretar in direktorji organizacijskih enot v Banki Slovenije,
- c) zaposleni v Banki Slovenije, ki jih pooblašćene osebe iz točke a) ali točke b) tega odstavka za to pisno pooblastijo.

(3) Pooblašćene osebe iz točke c) prejšnjega odstavka pooblastila ne morejo prenesti na drugo osebo.

(4) Stopnjo zaupnosti »BSI-ZAUPNO« lahko za dokumente oziroma druge nosilce podatkov Banke Slovenije dodeli izključno:

- član Sveta Banke Slovenije in
- generalni sekretar in direktorji organizacijskih enot v Banki Slovenije, za informacije s področja dela te organizacijske enote.

(5) Stopnjo zaupnosti »BSI-TAJNO« lahko za informacije Banke Slovenije določi izključno član Sveta Banke Slovenije.

(6) Pooblašćena oseba Banke Slovenije določi stopnjo zaupnosti dokumenta, ki vsebuje zaupne informacije Banke Slovenije, ob podpisu dokumenta.

(7) Pooblašćena oseba Banke Slovenije, ki na dokumentu določi stopnjo zaupnosti »BSI-TAJNO« ali »BSI-ZAUPNO«, mora stopnjo zaupnosti preklicati oziroma prilagoditi, če pri informaciji niso več izpolnjeni kriteriji za takšno stopnjo zaupnosti. Če je mogoče, mora oznaka zaupnosti vsebovati informacijo, kdaj se zaupnost lahko zniža (npr. na doloćen datum ali ob nastopu doloćenega dogodka) in na katero raven (npr. »BSI-TAJNO do [datum ali dogodek], zatem BSI-ZAUPNO«, ali »BSI-ZAUPNO do [datum ali dogodek], zatem BSI-OMEJENO«).

7. člen
(obravnavo zaupnih informacij drugega subjekta)

(1) Zaupne informacije drugih subjektov v Republiki Sloveniji, druge države ali institucij Evropske unije oziroma mednarodnih organizacij, ki jih prejme Banka Slovenije, se obravnavajo v skladu s stopnjo zaupnosti, doloćeno v skladu s tem sklepom, ki je primerljiva s stopnjo zaupnosti, ki jo je določil ta subjekt ali institucija ali mednarodna organizacija, da se zagotavlja enakovredno varovanje zaupnosti. Z nižjo stopnjo zaupnosti se lahko zaupne informacije drugega subjekta obravnavajo le na podlagi pridobljenega pisnega soglasja tega subjekta ali institucije ali mednarodne organizacije. Dokumenti praviloma ohranijo oznake, ki so v rabi v tem subjektu ali instituciji ali mednarodni organizaciji, lahko pa se dodatno oznaćijo z oznako zaupnosti v skladu s tem sklepom.

(2) Primerljive stopnje in oznake stopenj zaupnosti so primeroma navedene v prilogi 2 tega sklepa.

8. člen

(označevanje zaupnih informacij na dokumentu ali drugem nosilcu podatkov)

(1) Vsak dokument, ki vsebuje zaupne informacije Banke Slovenije, mora biti ob določitvi stopnje zaupnosti vidno označen z ustrezno oznako stopnje zaupnosti v skladu s tem sklepom.

(2) Dokumenti, ki vsebujejo zaupne informacije Banke Slovenije, morajo imeti na vseh straneh dokumenta v zgornjem desnem kotu označeno stopnjo zaupnosti. Vsaka stran dokumenta z oznako stopnje zaupnosti mora imeti v spodnjem delu strani navedeno tudi številko strani, glede na skupno število strani dokumenta (npr. stran 3 od 7).

(3) Na prvi strani dokumenta, ki vsebuje zaupne informacije Banke Slovenije, se pod oznako stopnje zaupnosti lahko doda dodatna oznaka, s katero se pojasni: razlog za dodeljeno stopnjo zaupnosti (npr. »osebni podatki«), obseg seznanitve z zaupno informacijo (npr. »za naslovnika«) ali čas trajanja opredeljene stopnje zaupnosti (npr. »BSI-ZAUPNO do [datum ali dogodek], zatem BSI-OMEJENO«).

(4) Oznaka zaupnosti na nosilcu podatkov, ki vsebuje zaupne informacije Banke Slovenije, mora biti na nosilcu podatkov vidno natiskana, napisana, naslikana, nalepljena ali kako drugače pritrjena s primernimi sredstvi. Označevanje nosilca podatkov ne sme uničiti ali poškodovati zaupne informacije Banke Slovenije oziroma povzročiti, da ta postane neuporabna.

(5) Če se dokumente ali druge nosilce podatkov, ki vsebujejo zaupne informacije Banke Slovenije, združuje, mora biti zbirka označena s stopnjo zaupnosti, ki ustreza najvišji stopnji zaupnosti informacij, ki so vključene v posamezen dokument ali shranjene na posameznem nosilcu podatkov. Zbirka informacij je lahko razvrščena višje kot njeni sestavni deli.

(6) Sistem, v katerem se obdelujejo zaupne informacije Banke Slovenije, mora imeti vgrajen mehanizem, ki ob prikazu ali iznosu zaupne informacije iz sistema uporabnika seznani s stopnjo zaupnosti. V primeru, da sistem ne omogoča prikaza stopnje zaupnosti posamezne informacije, mora upravitelj sistema zagotoviti, da se uporabnik sistema ob vsakokratni prijavi v sistem nedvoumno seznani z najvišjo stopnjo zaupnosti informacij, ki se lahko obdelujejo v sistemu.

(7) Po presoji pooblaščen osebe, kot je opredeljena v 6. členu tega sklepa, se ob iznosu dokumenta, ki vsebuje zaupne informacije Banke Slovenije iz sistema, v katerem se obdeluje, na vsako stran dokumenta lahko doda vodni žig, ki vsebuje: datum in čas iznosa, stopnjo zaupnosti in oznako prejemnika.

(8) Dokument ali drug nosilec podatkov, ki vsebuje zaupne informacije Banke Slovenije in ki ga Banka Slovenije posreduje zunanjim prejemnikom, se lahko označi z oznako enakovredne stopnje zaupnosti iz priloge 2 tega sklepa, ki jo uporablja zunanji prejemnik in ki zagotavlja enakovredno varnost kot dodeljena stopnja zaupnosti v Banki Slovenije.

9. člen

(trajanje zaupnosti)

(1) Zaupni informaciji Banke Slovenije zaupnost preneha:

- na določen datum ali s potekom določenega časa ali z nastopom določenega dogodka, ki je določen za spremembo stopnje zaupnosti ali
- s preklicem zaupnosti.

(2) Za dokumente in druge nosilce podatkov, ki so označeni s stopnjami zaupnosti Banke Slovenije »BSI-TAJNO« in »BSI-ZAUPNO«, se praviloma dve leti po določitvi stopnje zaupnosti, za informacije s stopnjo zaupnosti »BSI-OMEJENO« pa na vsakih šest let po določitvi stopnje zaupnosti, stopnja zaupnosti zniža za eno stopnjo, do stopnje »BSI-NEJAVNO«, razen če pooblaščen oseba

Banke Slovenije po poteku posameznega obdobja izrecno zavrne spremembo stopnje zaupnosti zaradi učinkovitega obvladovanja tveganj v zvezi z določbami predpisov ali pravil drugih subjektov v Republiki Sloveniji, drugih držav ali institucij Evropske unije ali mednarodnih organizacij, ki so informacijo pripravile. V primeru zavrnitve se uporaba veljavne stopnje zaupnosti podaljša za dodatno obdobje. Banka Slovenije lahko določi postopek zniževanja stopenj zaupnosti za sorodne skupine dokumentov.

(3) Zaupnost informacij v dokumentih ali drugih nosilcih podatkov Banke Slovenije v vsakem primeru preneha s potekom časa, ki je določen v zakonu, ki ureja arhivsko gradivo in arhive.

(4) Poleg primerov iz prvega odstavka, pooblaščen oseba Banke Slovenije na podlagi ocene negativnega vpliva prekliche ali spremeni oznako stopnje zaupnosti dokumenta ali drugega nosilca podatkov, če ob ponovni uporabi dokumenta ali drugega nosilca podatkov ugotovi, da niso več podani pogoji za ohranitev stopnje zaupnosti informacij.

(5) Pooblaščen oseba Banke Slovenije mora za zaupne informacije Banke Slovenije, ki jim je določena stopnja zaupnosti »BSI-TAJNO« ali »BSI-ZAUPNO« ali »BSI-OMEJENO«, ob vsakem posredovanju ponovno oceniti, ali dodeljena stopnja zaupnosti še ustreza stopnji negativnega vpliva, glede na okoliščine, ki obstajajo v času ponovne ocene, zlasti ob upoštevanju poteka časa.

(6) Kadar je to glede na okoliščine primerno, Banka Slovenije o preklicu oziroma znižanju stopnje zaupnosti na dokumentih ali nosilcih podatkov s stopnjo oznake zaupnosti »BSI-TAJNO« ali »BSI-ZAUPNO« ali »BSI-OMEJENO«, obvesti vse zunanje prejemnike, ki jim je dokument posredovala.

10. člen **(predlog za preklic zaupnosti)**

Pravna ali fizična oseba, ki ji je Banka Slovenije zavrnila zahtevo za dostop ali razkritje informacije ali dokumenta zaradi zaupnosti informacije, lahko Banki Slovenije predlaga preklic stopnje zaupnosti informacije oziroma dokumenta. O predlogu z upoštevanjem 7. člena tega sklepa odloči pooblaščen oseba.

III. POGLAVJE **UKREPI IN POSTOPKI ZA VAROVANJE ZAUPNIH INFORMACIJ**

11. člen **(splošni ukrepi)**

Osebe, ki pridobijo ali razpolagajo z zaupnimi informacijami Banke Slovenije (prejemniki zaupnih informacij), morajo:

- upoštevati določbe tega sklepa ter veljavnih predpisov in pogodbenih obveznosti v zvezi z varovanjem teh informacij,
- zagotoviti, da se s temi informacijami seznanijo zgolj tiste pooblaščen osebe pri prejemniku, ki te informacije potrebujejo za izvajanje nalog pri doseganju namena, zaradi katerega so bile te informacije pridobljene,
- te informacije uporabiti v skladu s predpisi in izključno za namen, za katerega so jim bile posredovane,
- zagotoviti ustrezne tehnične in organizacijske ukrepe, kot so opredeljeni v 12. členu tega sklepa, da se zagotovi varnost teh informacij ter prepreči nepooblaščen razkritje ali uporaba teh informacij v nasprotju z veljavnimi predpisi. V primeru, da ne morejo zagotoviti ukrepov, ki so opredeljeni kot obvezni, morajo te informacije nemudoma izbrisati.

12. člen

(tehnični in organizacijski ukrepi)

(1) Zagotovljena morata biti stalni nadzor nad zaupnimi informacijami Banke Slovenije ter ustrezno varovanje pred nepooblaščenim dostopom, spremembo ali uničenjem.

(2) Minimalni nabor tehničnih in organizacijskih ukrepov za varnost zaupnih informacij Banke Slovenije vključuje ukrepe, ki so za posamezno stopnjo zaupnosti določeni v prilogi 3 tega sklepa.

(3) Banka Slovenije lahko v posameznih primerih za obdelavo zaupnih informacij Banke Slovenije določi dodatne ukrepe in pogoje, ki morajo biti izpolnjeni pred začetkom obdelave.

13. člen

(posredovanje zaupnih informacij)

(1) Banka Slovenije posreduje zaupne informacije zunanjemu prejemniku:

– če zakon izrecno določa obveznost posredovanja zaupnih informacij določenemu prejemniku, ali

– če je v skladu z zakonom posredovanje določenih zaupnih informacij nujno zaradi izvajanja pristojnosti in nalog, ki jih zakon nalaga Banki Slovenije, ali

– kadar je posredovanje zaupnih informacij prejemniku nujno zaradi varstva zakonitih interesov zunanjega prejemnika, razen kadar javni interes glede varstva zaupnosti v konkretnem primeru prevlada nad zakonitimi interesi posameznega prejemnika, ali

– če je v skladu z zakonom in pogodbo o posredovanju, ki jo sklene Banka Slovenije z zunanjim prejemnikom, posredovanje zaupnih informacij potrebno zaradi učinkovitega izvajanja zakonskih nalog in pristojnosti Banke Slovenije ali drugega poslovanja Banke Slovenije.

(2) Ne glede na prejšnji odstavek, Banka Slovenije ne posreduje zaupnih informacij zunanjemu prejemniku, kadar zakon izrecno prepoveduje posredovanje določenih informacij.

(3) Zahteva za posredovanje zaupnih informacij, ki jo na Banko Slovenije naslovi zunanji prejemnik, se predloži v pisni obliki in mora vsebovati:

- podatke o vlagatelju ter podpis vlagatelja oziroma pooblaščene osebe,
- pravno podlago za pridobitev zahtevanih zaupnih informacij,
- namen oziroma razloge, ki izkazujejo potrebnost in primernost zaupnih informacij za dosego namena pridobitve,
- predmet ali številko ali drugo identifikacijo zadeve, v zvezi s katero so zaupne informacije potrebne,
- zaupne informacije, ki naj se posredujejo,
- obliko in način pridobitve zahtevanih zaupnih informacij.

(4) Posredovanje zaupnih informacij zunanjemu prejemniku je dovoljeno izključno na podlagi predhodne pisne odobritve pooblaščene osebe Banke Slovenije:

- za informacije z oznakami zaupnosti »BSI-NEJAVNO« presodi zaposleni sam,
- za informacije z oznakami zaupnosti »BSI-OMEJENO« presodi generalni sekretar ali direktor organizacijske enote, ki je odgovorna za informacijo,
- za informacije z oznakami zaupnosti »BSI-ZAUPNO« presodi pristojni član Sveta Banke Slovenije, ali po pooblastilu guvernerja generalni sekretar,
- za informacije z oznakami zaupnosti »BSI-TAJNO« presodi guverner, ali oseba, ki jo ta izrecno pooblasti za posredovanje oziroma odobritev posredovanja informacij v konkretnih zadevi.

(5) Za zaupne informacije, ki jih Banka Slovenije pridobi od zunanjih subjektov (v nadaljevanju: izvorni subjekt), Banka Slovenije pred posredovanjem teh zaupnih informacij zunanjim prejemnikom pridobi stališče izvirnega subjekta glede posredovanja, razen če je takšno obveščanje izvirnega subjekta z zakonom izrecno prepovedano. Banka Slovenije glede posredovanja informacij zunanjemu

prejemniku upošteva stališče izvirnega subjekta, razen če je posredovanje konkretnih zaupnih informacij določeno z zakonom, ki zavezuje Banko Slovenije. Če v tem primeru izvorni subjekt nasprotuje posredovanju, Banka Slovenije uporabi razpoložljiva pravna sredstva, da ugovarja zahtevi zunanjega prejemnika.

(6) Banka Slovenije zunanjega prejemnika zaupnih informacij opozori na stopnjo zaupnosti, ki je dodeljena zaupnim informacijam, in dolžnost zunanjega prejemnika glede varovanja zaupnosti teh informacij v skladu s tem sklepom in morebitnimi dodatnimi pogoji za zagotavljanje varstva zaupnosti informacij. Zunanji prejemnik mora pri posredovanju zaupnih informacij drugemu prejemniku upoštevati veljavne predpise in zakonitost namenov ter o posredovanju informacij stopnje zaupnosti »BSI-TAJNO« ali »BSI-ZAUPNO« obvestiti Banko Slovenije.

(7) Kadar je to primerno glede na konkretne okoliščine in naravo zaupnih informacij, lahko Banka Slovenije v zvezi s posredovanjem zaupnih informacij od zunanjega prejemnika zahteva, da z Banko Slovenije sklene sporazum o varovanju zaupnosti, ki je lahko del pogodbe o posredovanju podatkov.

14. člen **(obveščanje o kršitvah varovanja zaupnosti)**

Osebe, ki pridobijo ali razpolagajo z zaupnimi informacijami Banke Slovenije, morajo v primeru zaznanih kršitev varovanja zaupnih informacij, zaradi katerih je prišlo do izgube ali razkritja zaupne informacije nepooblaščenim osebam, o tem nemudoma obvestiti Banko Slovenije in ukreniti vse potrebno, da se odpravijo škodljive posledice in prepreči ponovna izguba ali nepooblaščen razkritje zaupnih informacij Banke Slovenije. Iz obvestila morajo biti razvidni: identifikacija zaupne informacije, posredovalni subjekt in prejemnik, okoliščine in obseg kršitve ter izvedeni ukrepi.

IV. POGLAVJE **PREHODNE IN KONČNE DOLOČBE**

15. člen **(uveljavitev sklepa)**

(1) Ta sklep začne veljati 1. 3. 2027.

(2) Z dnem uveljavitve tega sklepa preneha veljati Pravilnik o varovanju zaupnih podatkov Banke Slovenije z dne 3. 9. 2019.

(3) Oznake zaupnosti na dokumentih, ki so bili ustvarjeni do uveljavitve tega sklepa, se po njegovi uveljavitvi uporabljajo v vsebini, kot izhaja iz Priloge 2, ter se nadomestijo z novimi oznakami zaupnosti v skladu z določili iz drugega odstavka 9. člena sklepa.

Št. 009/2026

Ljubljana, dne 6. oktobra 2026

EDA 2026-5023912000-0010

Primož Dolenc
predsednik
Sveta Banke Slovenije

KRITERIJI ZA DOLOČANJE NEGATIVNEGA VPLIVA NA DELOVANJE BANKE SLOVENIJE (BS)

RAZVRSTITEV	OPIS POSLEDIC Nepooblaščen dostop ali razkritje informacij bi lahko imel naslednje negativne posledice:
BS-JAVNO	Informacija ki je bodisi že bila javno razkrita bodisi njeno razkritje ne bi imelo negativnega vpliva na delovanje BS.
BSI-NEJAVNO	Verjetno negativen vpliv na delovanje BS predvsem zaradi: • nedoseganja internih pričakovanj BS; • začasnega vznemirjenja na trgih in neželenih tržnih gibanj v enem dnevu; • finančne izgube od 10.000 EUR do 100.000 EUR.
BSI-OMEJENO	Verjetno POMEMBEN negativen vpliv na delovanje BS (ESCB/EMN/EMR) predvsem zaradi: • nezadovoljive kakovosti ali večje zamude pri izvajanju statutarnih nalog ali delnega neuspeha pri doseganju strateških ciljev; • vznemirjenja na trgih in neželenih večjih tržnih gibanj v enem dnevu; • finančne izgube nad 100.000 EUR in do 1.000.000 EUR; • težav za posamezno osebo; • kršitve statutarnih/regulativnih omejitev glede razkritja informacij; • kršitve dolžnosti skrbnega ravnanja pri varovanju zaupnosti informacij, ki jih posredujejo tretje osebe.
BSI- ZAUPNO	Verjetno RESEN negativen vpliv na delovanje BS (ESCB/EMN/EMR) predvsem zaradi: • delnega neuspeha pri izvajanju statutarnih nalog ali neuspeha pri izvajanju svetovalnih nalog ali popolnega neuspeha pri doseganju strateškega cilja; • neželenih negativnih reakcij trgov in neželenih večjih tržnih gibanj, ki trajajo od enega dne do enega tedna; • finančne izgube nad 1.000.000 EUR in do 10.000.000 EUR; • omogočanja posameznikom ali podjetjem, da pridobijo neupravičene prihodke ali koristi; • oviranja preiskave kaznivih dejanj ali omogočanja storitve kaznivih dejanj; • povzročanja hude težave ali škode konkretnim posameznikom.
BSI-TAJNO	Verjetno ZELO RESEN negativen vpliv na delovanje BS (ESCB/EMN/EMR) predvsem zaradi: • neizpolnitve zakonskih in statutarnih nalog in ciljev BS; • neželenih negativnih reakcij trgov in večjih neželenih tržnih gibanj, ki trajajo več kot en teden; • zelo velike škode za operativno učinkovitost Eurosistema; • hude škode za ključne interese Evropske unije ali države članice; • informacij o finančni krizi, ki bi lahko povzročile nadaljnjo destabilizacijo finančnih trgov; • finančne izgube nad 10.000.000 EUR.

OZNAKE ENAKOVREDNIH STOPENJ ZAUPNOSTI

BS – NOVE OZNAKE	BS – STARE OZNAKE	ESCB/EMN	SRB	EBA
BSI-JAVNO	BS-JAVNO	ECB-PUBLIC	SRB-GREEN	PUBLIC
BSI-NEJAVNO	BS-INTERNO	ECB-UNRESTRICTED	SRB-BLUE	EBA Regular use
BSI-OMEJENO	BS-ZAUPNO	ECB-RESTRICTED	SRB-YELLOW	EBA Restricted use
BSI-ZAUPNO	BS-STROGO ZAUPNO	ECB-CONFIDENTIAL	SRB-ORANGE	EBA Confidential use
BSI-TAJNO	BS-TAJNO	ECB-SECRET	SRB-RED	

**MINIMALNI TEHNIČNI IN ORGANIZACIJSKI UKREPI ZA VAROVANJE ZAUPNIH INFORMACIJ
BANKE SLOVENIJE**

Domena	Ukrep	BS-NEJAVNO	BS-OMEJENO	BS-ZAUPNO	BS-TAJNO
Upravljanje informacijske varnosti	Opredelitev internih aktov o zagotavljanju informacijske varnosti	-	-	P	P
	Imenovanje odgovorne osebe za informacijsko varnost	-	-	-	P
Varnost osebja	Pogodba o nerazkrivanju zaupnih informacij za zaposlene, zunanje sodelavce, pogodbenne partnerje	-	P	O	O
	Stroške kadrovske varnostne preverbe za osebe z dostopom.	-	-	-	P
Nadzor dostopa	Omejitev dostopa na pooblaščen uporabnike	P	O	O	O
	Odobritev dostopa po načelu potrebe po vedenju	P	O	O	O
	Evidentiranje vseh oseb z dostopom	P	O	O	O
	Redna revizija dostopov: najmanj enkrat letno	-	P	O	X
	Redna revizija dostopov: najmanj vsakih 6 mesecev	-	-	-	O
	Avtentikacija uporabnikov: uporabniško ime in geslo, vzpostavljena politika težko uganljivih gesel	O	O	X	X
	Avtentikacija uporabnikov: digitalna potrdila ali večfaktorska avtentikacija s programskim multifaktorskim avtentikatorjem	-	-	O	X
	Avtentikacija uporabnikov: večfaktorska avtentikacija s strojnimi multifaktorskim avtentikatorjem kombiniranim z geslom/PIN	-	-	-	O
Kriptografska zaščita	Šifrirni ključi izključno pod nadzorom organizacije	-	-	P	O
Fizična in okoljska varnost	Hramba fizičnih nosilcev podatkov: v zaklenjenih omarah/pisarniškem pohištvu	P	O	X	X
	Hramba fizičnih nosilcev podatkov: v varovanih prostorih s fizično kontrolo pristopa	-	-	O	O
Varnost operacij	Vzpostavljena zaščita pred škodljivo kodo	O	O	O	O
	Redno varnostno posodabljanje informacijskih sistemov in programske opreme	O	O	O	O
	Elektronsko beleženje vseh dostopov do zaupnih podatkov	-	-	P	O
	Beleženje vseh obdelav zaupnih podatkov	-	-	-	P
Varnost operacij	Vzpostavljen sistem za zaznavanje in preprečevanje vdorov	-	-	-	P
Varnost omrežij in komunikacij	Preverjanje verodostojnosti naprav priključenih v omrežje	-	P	P	O
	Šifriranje mrežnega prometa: znotraj organizacije	-	P	P	O

Domena	Ukrep	BS-NEJAVNO	BS-OMEJENO	BS-ZAUPNO	BS-TAJNO
	Šifriranje mrežnega prometa: zunaj organizacije	P	O	O	O
	Šifriranje mrežnega prometa: End-to-end šifriranje	-	-	P	O
	Šifriranje prenosa po elektronski pošti: znotraj organizacije		P	O	X
	Šifriranje prenosa po elektronski pošti: zunaj organizacije	P	O	O	X
Upravljanje dobaviteljev	Varnostne zahteve v pogodbah s ponudniki in dobavitelji	P	P	O	O
Upravljanje incidentov	Vzpostavljen postopek za odzivanje na incidente	-	P	P	O
	Vzpostavljeno redno spremljanje varnostnih dogodkov	-	-	P	O
Skladnost					
	Prepoved obdelave z uporabo javnih oblčnih storitev	-	-	P	O
	Prepoved obdelave z uporabo umetne inteligence	-	-	-	O
	Prepoved obdelave na mobilnih napravah	-	-	-	O
	Hramba in obdelava podatkov: izključno na ozemlju Republike Slovenije	-	-	P	O
	Omejitev v primeru hrambe in obdelave podatkov izven ozemlja Republike Slovenije: izključno na ozemlju druge države članice EU	-	P	O	X
Upravljanje podatkov	Zaščita s šifriranjem: v času hrambe na izmenljivih nosilcih podatkov in mobilnih napravah	O	O	O	X
	Zaščita s šifriranjem: v času hrambe v javnih oblčnih storitvah	P	O	O	X
	Zaščita s šifriranjem: v času hrambe na delovnih postajah	-	P	O	O
	Zaščita s šifriranjem: v času hrambe v lokalnih strežniških sistemih in bazah podatkov	-	-	P	O
	Brisanje: z overjenim orodjem /uničenje papirja	P	O	X	X
	Brisanje: z overjenim orodjem /uničenje papirja in z evidenco	-	-	O	O
Ozaveščanje in usposabljanje	Zagotovljeno redno usposabljanje zaposlenih o informacijski varnosti	P	P	O	O

Legenda:

O : Obvezno

P : Priporočeno

X : Ni dovoljeno¹

- : Ni predpisano

¹ Ni dovoljeno se ne nanaša na varnostni ukrep temveč na sam scenarij pri katerem naj bi se ukrep uporabil (npr. Zaščita s šifriranjem: v času hrambe v javnih oblčnih storitvah ne pomeni, da ni dovoljeno šifriranje temveč, da ni dovoljena hramba v javnih oblčnih storitvah).

