HNB
EUROSUSTAV

Trg hrvatskih velikana 3, HR-10000 Zagreb
T. +385 1 4564 555 · F. +385 1 4610 551
www.hnb.hr

Smjernice za izvješćivanje HNB-a o značajnim IKT incidentima i ozbiljnim kibernetičkim prijetnjama putem Nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima – Platforme PiXi

Zagreb, srpanj 2025.

HRVATSKA NARODNA BANKA
EUROSUSTAV

Regulatorni okvir

1. Uredba (EU) 2022/2554 o digitalnoj operativnoj otpornosti za financijski sektor[1] (u nastavku teksta: Uredba DORA) primjenjuje se od 17. siječnja 2025. te definira zahtjeve izvješćivanja o značajnim IKT incidentima i dobrovoljno izvješćivanja nadležnih tijela o ozbiljnim kibernetičkim prijetnjama.
2. Uredba DORA također harmonizira zahtjeve izvješćivanja prema nacionalnim nadležnim tijelima, europskima nadzornim tijelima, Europskoj središnjoj banci te jedinstvenim kontaktnim točkama ili timovima za odgovor na računalne sigurnosne incidente imenovanima ili uspostavljenima u skladu s Direktivom (EU) 2022/2555 (NIS2)[2]. S početkom primjene Uredbe DORA ukinuti su okviri za izvješćivanje o IKT incidentima definirani Odlukom o primjerenom upravljanju informacijskim sustavom[3], Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga[4], Zakonom o platnom prometu[5] i Revidiranim smjernicama o izvješćivanju o značajnim incidentima u skladu s Direktivom PSD2[6].
3. Prema članku 8. stavku 3. Zakona o provedbi Uredbe (EU) 2022/2554 o digitalnoj operativnoj otpornosti za financijski sektor[7] (u nastavku teksta: Zakona) Hrvatska narodna banka (u nastavku teksta: HNB) jest nadležno tijelo i provodi nadzor nad sljedećim subjektima (u nastavku teksta: subjekt nadzora): kreditnim insitucijama, institucijama za platni promet, pružateljima usluga informiranja o računu, institucijama za elektronički novac, pružateljima usluga informiranja o računu i izdavateljima tokena vezanih uz imovinu.
4. Radi uspostave izvješćivanja o značajnim IKT incidentima i ozbiljnim kibernetičkim prijetnjama, subjekti nadzora primjenjuju odredbe definirane „poglavljem III. – Upravljanje, klasifikacija i izvješćivanje u vezi s IKT incidentima“ Uredbe DORA, Delegiranom Uredbom komisije (EU) 2024/1772[8] (u nastavku teksta: RTS za

[1] Uredba (EU) 2022/2554 o digitalnoj operativnoj otpornosti za financijski sektor, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32022R2554
[2] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2)
[3] Odluka o primjerenom upravljanju informacijskim sustavom (NN, br. 110/2022. i 152/2024.)
[4] Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN, br. 64/2018.)
[5] Zakon o platnom prometu (NN, br. 66/2018., 114/2022. i 136/2024.)
[6] Revidirane smjernice o izvješćivanju o značajnim incidentima u skladu s Direktivom PSD2 (EBA/GL/2021/03)
[7] Zakon o provedbi Uredbe (EU) 2022/2554 o digitalnoj operativnoj otpornosti za financijski sektor (NN, br. 136/2024.), https://narodne-novine.nn.hr/clanci/sluzbeni/2024_11_136_2242.html
[8] Delegirana Uredba komisije (EU) 2024/1772 od 13. ožujka 2024. o dopuni Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda kojima se utvrđuju kriteriji za klasifikaciju IKT incidenata i kiberprijetnji, pragovi značajnosti i pojedinosti izvješća o značajnim incidentima

klasifikaciju) i Delegiranom uredbom Komisije (EU) 2025/301[9] (u nastavku teksta: RTS za sadržaj izvješća).

5. Prema članku 14. Zakona, subjekti iz članka 8. stavka 3. Zakona **dužni su o značajnim IKT incidentima izvještavati HNB te Nacionalni CERT, a prema članku 15. Zakona subjekti su dužni izvještavati putem nacionalne platforme** za **prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima koja je uspostavljena zakonom kojim se uređuje kibernetička sigurnost (u nastavku teksta: PiXi platforma).** Također, putem Platforme PiXi subjekti mogu na dobrovoljnoj osnovi izvještavati i o ozbiljnoj kibernetičkoj prijetnji.
6. Člankom 19. Zakona propisane su prekršajne odredbe vezane uz neispunjavanje obveza izvješćivanja o značajnim IKT incidentima.

Cilj Smjernica

7. Ovim Smjernicama, u skladu s člankom 15. stavkom 3. Zakona, određuju se pojedinosti u svezi s izvješćivanjem o značajnim IKT incidentima i ozbiljnim kibernetičkim prijetnjama putem Platforme PiXi.
8. Smjernicama se utvrđuje okvir za pristup Platformi PiXi od strane subjekata nadzora, pravila i postupci izvješćivanja te postupanje u slučaju kada korištenje Platforme PiXi nije moguće te se primjenjuju alternativni načini izvješćivanja.

Definicije

9. Osim ako nije drugačije navedeno, pojmovi korišteni i definirani Uredbom DORA imaju isto značenje kao u ovim Smjernicama.

Pristup Platformi PiXi

10. Pristup Platformi PiXi omogućen je subjektima nadzora.
11. Pristup Platformi PiXi ostvaruje se korištenjem Nacionalnoga identifikacijskoga i autentifikacijskog sustava (NIAS), u skladu s tehničkim uputama koje je objavio CARNET. Detaljan opis pristupa putem NIAS-a dostupan je u dokumentu Upute za pristup Platformi PiXi, objavljenom na početnoj stranici Platforme PiXi: https://pixi.carnet.hr/.

[9] Delegirana uredba Komisije (EU) 2025/301 od 23. listopada 2024. o dopuni Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda kojima se utvrđuju sadržaj i rokovi za početnu obavijest, prijelazno i završno izvješće o značajnim IKT incidentima te sadržaj dobrovoljne obavijesti o ozbiljnim kiberprijetnjama

Imenovanje osoba ovlaštenih za pristup Platformi PiXi

12. Subjekt nadzora imenuje osobu odgovornu za upravljanje korisničkim računima na Platformi PiXi (u nastavku teksta: administrator). Administrator mora biti zaposlenik subjekta nadzora. Subjekt nadzora može imenovati najviše dva administratora.
13. Subjekt nadzora imenuje osobe ovlaštene za izvješćivanje o značajnim IKT incidentima i ozbiljnim kiberntičkim prijetnjama putem Platforme PiXi (u nastavku teksta: korisnici Platforme PiXi). Korisnici Platforme PiXi mogu biti zaposlenici subjekta nadzora ili zaposlenici trećih strana pružatelja IKT usluga. Subjekt nadzora uvijek ostaje odgovoran za pravodobno i cjelovito izvješćivanje o značajnim IKT incidentima.

Prava pristupa Platformi PiXi

14. Administrator operativno dodjeljuje i ukida prava pristupa korisnicima Platforme PiXi. Administrator može biti i korisnik Platforme PiXi.
15. Korisnici Platforme PiXi, u skladu s pravima pristupa koja su im dodijeljena, ovlašteni su unositi izvješća o značajnim IKT incidentima i ozbiljnim kibernetičkim prijetnjama.

Pravila korištenja Platforme PiXi

16. Korištenje Platforme PiXi provodi se u skladu s ovim Smjernicama i važećim Uvjetima korištenja Platforme PiXi, objavljenima na web-stranici: https://pixi.carnet.hr/.

Izvješćivanje putem Platforme PiXi

17. Ako subjekt nadzora na osnovi provedene klasifikacije u skladu s kriterijima iz RTS-a za klasifikaciju utvrdi da je IKT incident značajan ili da je kibernetička prijetnja ozbiljna, ispunjava na engleskom jeziku odgovarajući obrazac ESA. Obrazac ESA dostupan je na mrežnoj stranici HNB-a (poglavlje Smjernice i obrasci): https://www.hnb.hr/temeljne-funkcije/supervizija/digitalna-operativna-otpornost.
18. Popunjeni obrazac ESA dostavlja se putem Platforme PiXi u rokovima definiranima RTS-om za sadržaj izvješća. Detaljan postupak dostave izvješća putem Platforme PiXi opisan je u dokumentu Korisničke upute za Platformu PiXi (obveznici Uredbe DORA), dostupnom u zaštićenom dijelu Platforme PiXi nakon prijave u sustav: https://pixi.carnet.hr/.

Alternativni način izvješćivanja o značajnim IKT incidentima i ozbiljnim kibernetičkim prijetnjama

19. U iznimnim slučajevima kada – zbog opravdanih razloga – nije moguće koristiti se Platformom PiXi, subjekt nadzora izvješća dostavlja putem HNB-ova sustava sigurne razmjene, na način opisan u Prilogu 2. ovih Smjernica.

Ukidanje pristupa Platformi PiXi

20. HNB obavještava subjekt nadzora o ukidanju pristupa Platformi PiXi.
21. Ukidanje pristupa Platformi PiXi za pojedini subjekt nadzora provodi CARNET na zahtjev HNB-a.

Prijelazna odredba

22. Ove Smjernice primjenjuju se od 14. srpnja 2025., kada počinje obveza izvještavanja značajnih IKT incidenata i dobrovoljna prijava ozbiljnih kibernetičkih prijetnji putem Platforme PiXi od strane subjekata nadzora. S istim datumom, prestaju se primjenjivati Smjernice za izvješćivanje o značajnim IKT incidentima koje je HNB okružnicom dostavio svim subjektima Uredbe DORA od 15. siječnja 2025.

Prilog 1. Alternativni način izvješćivanja o značajnim IKT incidentima

U iznimnim slučajevima – kad dostava izvješća o značajnim IKT incidentima nije moguća putem PiXi Platforme – subjekti nadzora izvještavaju HNB o značajnom IKT incidentu na sljedeći način:

1. Nakon provedene klasifikacije primjenom kriterija iz RTS-a, subjekt izvješćuje HNB o značajnom IKT incidentu, dostavljanjem popunjenog obrasca ESA. Obrazac ESA dostupan je na HNB-ovoj mrežnoj stranici (poglavlje Smjernice i obrasci): https://www.hnb.hr/temeljne-funkcije/supervizija/digitalna-operativna-otpornost.
2. Obrazac ESA popunjava se na engleskom jeziku.
3. Popunjeni obrazac dostavlja se u rokovima definiranima RTS-om, na HNB-ov sustav za sigurnu razmjenu u mapu "<Naziv subjekta nadzora> – DSIS/DORA/" .
4. Za značajne IKT incidente potrebno je pridržavati se sljedeće konvencije imenovanja datoteke:
   DORA_Incident_report -<godina>-<interni ID incidenta>-<verzija>-<LEI kod>.xlsx
   Opis polja:
   - godina: dvoznamenkasti kôd koji označuje godinu klasifikacije incidenta
   - interni ID incidenta: znakovni kôd do najviše 15 znakova koji označuje referentni identifikator značajnog incidenta koji je odredio subjekt nadzora (u skladu s poljem 2.1 iz RTS/ITS za sadržaj izvješća). Moguće je koristiti se i kraćim kodovima (npr. od pet znamenki kao što je navedeno u sljedećim primjerima)
   - verzija: dvoznamenkasti kôd koji označuje sekvenciju dostavljanja datoteke za pojedini incident/prijetnju. Primjerice:
     - subjekt nadzora dostavlja prvi dokument (koji obično sadržava početnu obavijest značajnog IKT incidenta): verzija = 1
     - subjekt nadzora dostavlja prijelazno izvješće ili nadopunjenu obavijest: verzija = 2
     - svaka sljedeća dostava, bez obzira na to je li riječ o nadopunjenim izvješćima, višestrukim prijelaznim izvješćima ili završnom izvješću, uvećava verziju za 1
   - Kôd LEI: jedinstveni dvadesetznakovni kôd LEI (engl. *Legal Entity Identifier*) subjekta nadzora.

   Primjeri naziva datoteka (ovisno o sekvenciji dostave obrazaca s različitim tipovima izvješća):
   - dostava početnog izvješća značajnog IKT incidenata u 2025. godini (verzija = 1): *DORA_Incident_report-25-IR001-01-EXMPL02SAVSQ5M5LQO30.xlsx*
   - dostava prijelaznog izvješća (nakon prvotne dostave početnog): *DORA_Incident_report-25-IR001-02-EXMPL02SAVSQ5M5LQO30.xlsx*

- dostava završnog izvješća, nakon početnog i dva prijelazna izvješća (ukupno četvrta dostava):
  DORA_Incident_report-25-IR001-04-EXMPL02SAVSQ5M5LQO30.xlsx

5. Uoči ili odmah nakon dostave obavijesti/izvješća, potrebno je poslati i elektroničku poruku na elektroničku adresu DORA.reporting@hnb.hr s naslovom:

   a. „Incident Report-<Naziv subjekta nadzora>", ako izvješćujete o značajnom IKT incidentu
   b. „Cyber Threat-<Naziv subjekta nadzora>", ako izvješćujete o ozbiljnoj kibernetičkoj prijetnji.

Napomena:. U slučaju nemogućnosti pristupa postojećih korisnika ili potrebe za pristupom dodatnih korisnika HNB-ovu sustavu razmjene, potrebno je obavijestiti HNB i dostaviti zahtjev na elektroničku adresu DORA.reporting@hnb.hr