

EBA/GL/2025/02

11.2.2025

Riktlinjer

om ändring av riktlinjerna EBA/2019/04
för hantering av IKT-risker och
säkerhetsrisker

1. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer som har utfärdats enligt artikel 16 i förordning (EU) nr 1093/2010¹. I enlighet med artikel 16.3 i förordning (EU) nr 1093/2010 ska de behöriga myndigheterna och finansinstituten med alla tillgängliga medel söka följa riktlinjerna.
2. Av riktlinjerna framgår EBA:s syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn och på hur unionslagstiftningen ska tillämpas inom ett särskilt område. Behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010 som berörs av riktlinjerna ska följa dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sina rättsliga ramar eller tillsynsrutiner), även när riktlinjerna i första hand riktas till institut.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 ska de behöriga myndigheterna meddela EBA att de följer eller tänker följa dessa riktlinjer, eller i annat fall, senast den 20.05.2025, ange skälen till att de inte gör det. Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningar ska lämnas på det formulär som tillhandahålls på EBA:s webbplats med hänvisningen "EBA/GL/2025/02". Anmälningar ska lämnas in av personer som har befogenhet att rapportera om hur reglerna efterlevs på de behöriga myndigheternas vägnar. Eventuella förändringar av efterlevnadsstatus måste också rapporteras till EBA.
4. Anmälningarna kommer att offentliggöras på EBA:s webbplats i enlighet med artikel 16.3.

¹ Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

2. Målgrupp

5. Dessa riktlinjer är avsedda för behöriga myndigheter enligt definitionen i artikel 4.2 vii i förordning (EU) nr 1093/2010 och för finansinstitut enligt definitionen i artikel 4.1 i förordning (EU) nr 1093/2010, det vill säga betaltjänstleverantörer enligt artikel 1.1 i direktiv (EU) 2015/2366².

3. Genomförande

Tillämpningsdatum

6. Dessa riktlinjer börjar gälla senast den 20.05.2025.

4. Ändringar

7. Riktlinjerna EBA/GL/2019/04 ska ändras på följande sätt:
8. Syftet, som anges i punkterna 5 och 6, ersätts med följande:

”Dessa riktlinjer härrör från mandatet att utfärda riktlinjer enligt artikel 95.3 i direktiv (EU) 2015/2366 och omfattar aspekter av hanteringen av relationer med betalningsanvändare.”

Dessa riktlinjer kompletterar riskhanteringsåtgärderna enligt förordningen om digital operativ motståndskraft för finanssektorn (DORA-förordningen) och de tillhörande tekniska tillsynsstandarder som betaltjänstleverantörer som avses i punkt 5 ovan måste följa, i enlighet med artikel 95.1 i andra betaltjänstdirektivet, för att hantera operativa risker och säkerhetsrisker i samband med de betaltjänster som de tillhandahåller.
9. Det tillämpningsområde som anges i punkterna 7 och 8 utgår.

² Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (EUT L 337, 23.12.2015, s. 35).

”Dessa riktlinjer anger kraven för att fastställa, genomföra och kontrollera de säkerhetsåtgärder som betaltjänstleverantörer måste vidta i enlighet med artikel 95.1 i direktiv (EU) nr 2015/2366 för att hantera de operativa riskerna och säkerhetsriskerna förknippade med betaltjänsterna de erbjuder.”

10. De mottagare som anges i punkt 9 ersätts med följande:

”Dessa riktlinjer är avsedda för behöriga myndigheter enligt definitionen i artikel 4.2 vii i förordning (EU) nr 1093/2010 och till finansinstitut enligt definitionen i artikel 4.1 i förordning (EU) nr 1093/2010, det vill säga betaltjänstleverantörer enligt definitionen i artikel 1.1 a, b och d i direktiv (EU) 2015/2366, inbegripet fysiska eller juridiska personer som omfattas av ett undantag enligt artikel 32 eller 33 i direktiv (EU) 2015/2366 och juridiska personer som är undantagna enligt artikel 9 i direktiv 2009/110/EG³.”

11. De definitioner som anges i punkt 10 utgår.
12. Punkterna 1–91, som motsvarar avsnitten 3.1–3.7, utgår.

³ Europaparlamentets och rådets direktiv 2009/110/EG av den 16 september 2009 om rätten att starta och driva affärsverksamhet i institut för elektroniska pengar samt om tillsyn av sådan verksamhet, om ändring av direktiven 2005/60/EG och 2006/48/EG och om upphävande av direktiv 2000/46/EG (EUT L 267, 10.10.2009, s. 7).