

Finansinspektionens föreskrifter om verksamhet för betaltjänstleverantörer;

FFFS 2018:4

Utkom från trycket
den 23 april 2018

beslutade den 17 april 2018.

Finansinspektionen föreskriver¹ följande med stöd av 5 § 8–16 förordningen (2010:1008) om betaltjänster.

1 kap. Tillämpningsområde och definitioner

Tillämpningsområde

1 § Dessa föreskrifter gäller för följande betaltjänstleverantörer som tillhandahåller betaltjänster i Sverige

- kreditinstitut,
- betalningsinstitut,
- registrerade betaltjänstleverantörer,
- institut för elektroniska pengar, och
- registrerade utgivare av elektroniska pengar.

Bestämmelserna i 6 kap. 2 § gäller även för utländska betaltjänstleverantörer med filial i Sverige.

2 § Bestämmelserna i 4 kap. gäller endast för betaltjänstleverantörer som tillhandahåller betalkonton till konsumenter där konsumenten åtminstone kan

1. placera medel på ett betalkonto,
2. ta ut kontanter från ett betalkonto, och
3. utföra och ta emot betalningstransaktioner till och från tredjepart.

Definitioner

3 § I föreskrifterna har termer och uttryck samma betydelse som i lagen (2010:751) om betaltjänster. Därutöver avses med

riktighet: att information inte förändras obehörigen, av misstag eller på grund av funktionsstörning,

¹ 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, samt Europaparlamentets och rådets direktiv 2014/92/EU av den 23 juli 2014 om jämförbarhet för avgifter som avser betalkonto, byte av betalkonto och tillgång till betalkonto med grundläggande funktioner.

betalningsrelaterade tjänster: all affärsverksamhet som avses i artikel 4.3 i betaltjänstdirektivet och all teknisk support som behövs för ett korrekt tillhandahållande av betaltjänster,

integritet: ett säkerställande av att ett företags tillgångar, inklusive data, är korrekta och fullständiga,

konfidentialitet: förhållandet att information inte görs tillgänglig eller avslöjas för obehöriga,

kontinuitet: att de processer, uppgifter och tillgångar som en organisation behöver för att leverera betalningsrelaterade tjänster är fullt tillgängliga och fungerar på i förväg fastställda godtagbara nivåer,

mottagande betaltjänstleverantör: den betaltjänstleverantör som en konsument vill byta betalkonto till,

operativa incidenter eller säkerhetsincidenter: en enskild händelse eller en serie av sammanhängande händelser som inte har planerats av betaltjänstleverantören, vilka har eller sannolikt kommer att få negativa effekter på betalningsrelaterade tjänster vad gäller integritet, tillgänglighet, konfidentialitet, riktighet eller kontinuitet,

riskaptit: en nivå och inriktning på företagets risker som kan accepteras för att uppnå företagets strategiska mål,

säkerhetsrisk: risken för att otillräckliga eller felaktiga interna processer eller externa händelser, inklusive cyberattacker eller otillräcklig fysisk säkerhet, negativt påverkar tillgängligheten, integriteten eller konfidentialiteten i

- informations- och kommunikationstekniska system, eller
- den information som används för att tillhandahålla betaltjänsterna,

tillgänglighet: att betalningsrelaterade tjänster är tillgängliga och kan användas av betaltjänstanvändarna.

överlämnande betaltjänstleverantör: den betaltjänstleverantör som en konsument vill byta betalkonto från.

2 kap. Betaltjänstleverantörers hantering av klagomål

1 § En betaltjänstleverantör ska ha lämpliga och effektiva rutiner för att hantera och besvara en betaltjänstanvändares klagomål på verksamheten i de länder där leverantören tillhandahåller betaltjänster.

Betaltjänstleverantören ska besvara klagomålet på ett språk som är officiellt i det land där betaltjänsten tillhandahålls, och lämna det i pappersform till betaltjänstanvändaren, om leverantören och användaren inte kommer överens om något annat.

2 § En betaltjänstleverantör ska besvara en betaltjänstanvändares klagomål inom 15 bankdagar från och med den dag klagomålet tas emot.

Om betaltjänstleverantören på grund av särskilda skäl inte har möjlighet att lämna ett svar inom den tid som anges i första stycket, ska leverantören svara inom 35 bankdagar från det att klagomålet tas emot. I sådana fall ska leverantören, inom

den tid som anges i första stycket, informera betaltjänstanvändaren om när svaret kommer att lämnas och om de särskilda skäl som förseningen beror på.

3 kap. Information om tjänster, avgifter och rättigheter

Information till konsumenter

1 § Den information som en betaltjänstleverantör enligt 4 a kap. 5 § andra stycket lagen (2010:751) om betaltjänster ska hålla tillgänglig för konsumenter, ska finnas på betaltjänstleverantörens webbplats. Detsamma gäller för den broschyr om konsumenters rättigheter som finns på Finansinspektionens webbplats.

Informationen enligt första stycket ska även finnas i pappersform hos filialer, ombud och i de av leverantörens lokaler som är tillgängliga för konsumenter.

2 § Om information enligt 1 § finns tillgänglig på en betaltjänstleverantörs webbplats ska texten även göras tillgänglig för uppläsning. Sådan information som finns i lokaler ska även göras tillgänglig i punktskrift eller i annat format som gör den tillgänglig för personer med funktionsnedsättning.

4 kap. Rutiner för byte av betalkonto

Krav på rutiner för byte av betalkonto

1 § De rutiner för byte av betalkonto som en betaltjänstleverantör ska ha enligt 4 a kap. 6 § lagen (2010:751) om betaltjänster ska åtminstone uppfylla kraven i 3–10 §§.

2 § Bestämmelserna i 3–10 §§ ska tillämpas från och med att den mottagande betaltjänstleverantören har öppnat det nya betalkonto som bytet ska ske till.

Skyldigheter för den mottagande betaltjänstleverantören

3 § Ett byte av betalkonto ska börja med att alla som är innehavare av betalkontot skriftligen ger den mottagande betaltjänstleverantören i uppdrag att genomföra bytet och lämnar instruktioner för hur uppdraget ska utföras. Den mottagande betaltjänstleverantören ska se till att det är möjligt för en konsument att lämna uppdraget och instruktionerna på svenska om betaltjänstleverantören och konsumenten inte kommer överens om något annat.

4 § Den mottagande betaltjänstleverantören ska se till att konsumenten har möjlighet att lämna instruktioner om vilka autogiromedgivanden, inkommande betalningar och stående överföringar knutna till det gamla betalkontot som ska knytas till det nya.

Betaltjänstleverantören ska även se till att konsumenten kan lämna instruktioner om att eventuellt kvarstående saldo på betalkontot hos den överlämnande betaltjänstleverantören ska överföras, och att betalkontot därefter ska avslutas.

5 § Den mottagande betaltjänstleverantören ska se till att konsumenten har möjlighet att bestämma vilket datum som bytet av betalkonto ska inledas.

6 § Den mottagande betaltjänstleverantören ska, om inget annat har avtalats mellan leverantörerna, skicka uppdraget och instruktionerna enligt 3 och 4 §§ på svenska till den överlämnande betaltjänstleverantören, senast bankdagen efter det datum som bestäms enligt 5 §.

7 § Den mottagande betaltjänstleverantören ska se till att de autogiromedgivanden och stående överföringar som anges i instruktionerna är knutna till det nya betalkontot senast tre bankdagar efter det datum som bestäms enligt 5 §.

8 § Om konsumenten har gett den mottagande betaltjänstleverantören i uppdrag att avsluta betalkontot hos den överlämnande betaltjänstleverantören, eller att överföra ett kvarstående saldo, ska den mottagande betaltjänstleverantören informera den överlämnande betaltjänstleverantören om hur det kvarstående saldot ska överföras.

9 § Den mottagande betaltjänstleverantören ska inom tre bankdagar från det datum som bestäms enligt 5 §, informera konsumenten om de uppgifter som krävs för att göra inbetalningar till betalkontot.

Skyldigheter för den överlämnande betaltjänstleverantören

10 § Den överlämnande betaltjänstleverantören ska upphöra med stående överföringar och autogireringar inom tre bankdagar från det att leverantören har tagit emot konsumentens uppdrag om att upphöra med sådana.

Om kvarstående medel på betalkontot hos den överlämnande betaltjänstleverantören ska överföras, eller om betalkontot ska avslutas, ska det kvarstående saldot överföras inom tre bankdagar från det att konsumentens uppdrag har mottagits. Den överlämnande betaltjänstleverantören ska avsluta betalkontot inom tre bankdagar från det att leverantören har tagit emot konsumentens uppdrag om avslut.

5 kap. System för operativa risker och säkerhetsrisker

1 § Det system som en betaltjänstleverantör ska ha enligt 5 b kap. 1 § lagen (2010:751) om betaltjänster, ska vara anpassat för leverantörens verksamhet och bestå av ett ramverk av dokumenterade åtgärder som hanterar eller minskar risken för att operativa incidenter eller säkerhetsincidenter inträffar. Inom ramen för systemet ska leverantören åtminstone

1. definiera och tilldela de ansvarsfunktioner som leverantören bedömer är nödvändiga för att genomföra säkerhetsåtgärderna,
2. fastställa processer, rutiner och system för att identifiera, mäta, övervaka och hantera riskerna som är förknippade med leverantörens betaltjänstverksamhet,
3. göra en riskbedömning av betaltjänsterna och ta fram en beskrivning av de säkerhetsåtgärder som ska skydda betaltjänstanvändarna mot de risker som identifierats, bland annat mot bedrägerier och olaglig användning av känsliga uppgifter och personuppgifter,
4. ha en intern nivåbaserad modell för att hantera och kontrollera risker i betaltjänstverksamheten,

5. ta fram en beskrivning av hur leverantören säkerställer att de operativa riskerna och säkerhetsriskerna hanteras när den uppdrar åt någon annan att utföra en del av betaltjänstverksamheten,
6. fastställa en riskaptit för betaltjänstverksamheten samt inventera, klassificera och riskbedöma affärsfunktioner, processer och tillgångar som anses kritiska för verksamheten,
7. ta fram säkerhetsåtgärder som hanterar konfidentialitet, integritet och tillgänglighet för data och it-system, samt fysisk säkerhet och åtkomstkontroll,
8. se till att verksamheten övervakas för att identifiera oplanerade händelser som leder till operativa eller säkerhetsrelaterade incidenter samt hantera, följa upp och rapportera incidenterna,
9. ta fram en plan för kontinuitetshantering, som innefattar en beskrivning av hur verksamheten ska upprätthållas i olika scenarier och hur leverantören ska kommunicera i händelse av kris, testa kontinuitetsplanerna årligen och vid behov uppdatera dem,
10. ta fram och regelbundet testa kontrollrutiner som säkerställer att säkerhetsåtgärderna är uppdaterade och effektiva,
11. ta fram en hotbildsanalys för betaltjänstverksamheten och regelbundet utbilda personalen om hur den ska använda beredskapsplaner, kontinuitetsplaner och återställningsplaner och
12. ta fram och vid behov genomföra processer och rutiner för att vägleda och informera betaltjänstanvändarna om säkerhetsrisker och felmeddelanden som är relaterade till de tillhandahållna betaltjänsterna och betaltjänstanvändarnas möjligheter att avaktivera specifika betalningsfunktioner.

6 kap. Uppgifter till Finansinspektionen

Övergripande bedömning av operativa risker, säkerhetsrisker och åtgärder

1 § En betaltjänstleverantör ska årligen komma in till Finansinspektionen med en rapport som innehåller en aktuell och övergripande bedömning av de operativa risker och säkerhetsrisker som är förknippade med de betaltjänster som leverantören tillhandahåller, och en beskrivning av de säkerhetsåtgärder som leverantören genomfört för att hantera dessa risker. Rapporten ska även innehålla en bedömning av lämpligheten av de säkerhetsåtgärder som leverantören genomfört för att hantera dessa risker.

Rapporten ska komma in till Finansinspektionen senast den 21 februari.

Statistiska uppgifter om svikliga förfaranden

2 § En betaltjänstleverantör ska två gånger per år lämna statistiska uppgifter till Finansinspektionen om svikliga förfaranden som har ägt rum i samband med användningen av betaltjänster. Uppgifterna ska innehålla

1. total transaktionsvolym,

2. total transaktionsvolym relaterad till svikliga förfaranden, och
3. en redovisning av uppgifter enligt 1 och 2 uppdelat på
 - a) typ av betaltjänst,
 - b) aktuell autentiseringsmetod,
 - c) typ av svikligt förfarande, och
 - d) var transaktionen genomförts geografiskt.

Uppgifterna ska avse det senaste kalenderhalvåret och delas upp per kvartal. Leverantören ska lämna uppgifterna genom att använda de blanketter för rapportering som finns på Finansinspektionens webbplats. Uppgifterna ska ha kommit in till myndigheten senast den 21 februari respektive senast den 21 augusti.

Registrerade betaltjänstleverantörer och registrerade utgivare av elektroniska pengar ska lämna uppgifter enligt första stycket endast en gång per år, senast den 21 februari, genom att använda de blanketter för rapportering som finns på Finansinspektionens webbplats. Uppgifterna ska avse det senaste kalenderåret och vara uppdelade per kvartal.

3 § Uppgifter enligt 2 § ska omfatta svikliga förfaranden som är relaterade till genomförda betalningstransaktioner som

1. inte auktoriserats av betalaren,
2. betalaren nekar till att denne har auktoriserat, eller
3. genomförts genom att betalaren manipulerats.

Allvarliga operativa incidenter eller säkerhetsincidenter

4 § En betaltjänstleverantör ska rapportera till Finansinspektionen om en allvarlig operativ incident eller säkerhetsincident uppkommit i verksamheten. Leverantören ska när den rapporterar använda den blankett för allvarliga incidenter som finns tillgänglig på Finansinspektionens webbplats.

Uppgifterna ska lämnas enligt blankettens avsnitt A–C, på det sätt som närmare anvisas på Finansinspektionens webbplats

1. inom fyra timmar efter det att incidenten upptäckts (avsnitt A),
2. med uppdaterad information när det finns sådan och senast inom tre dagar från det att uppgifterna enligt 1 har kommit in (avsnitt B), och
3. senast två veckor efter det att verksamheten fungerar normalt igen (avsnitt C).

5 § En betaltjänstleverantör ska informera sina betaltjänstanvändare om det inträffar en allvarlig operativ incident eller säkerhetsincident som kan påverka deras ekonomiska intressen negativt. När en betaltjänstleverantör informerar betaltjänstanvändare ska följande krav tillgodoses:

1. Informationen ska vara tillgänglig för betaltjänstanvändaren på ett varaktigt medium även efter informationstillfället.
2. Betaltjänstleverantören ska uppmärksamma betaltjänstanvändaren på att det finns information om en allvarlig operativ incident eller säkerhetsincident som kan påverka betaltjänstanvändarens ekonomiska intresse negativt.

3. Vid utformningen av sådan kommunikation ska betaltjänstleverantören beakta vikten av säker kommunikation vars ursprung betaltjänstanvändaren kan kontrollera.

Uppgifter om avgifter för tjänster

6 § En betaltjänstleverantör som tillhandahåller betalkonton med grundläggande funktioner enligt 4 a kap. 2 § lagen (2010:751) om betaltjänster, ska lämna uppgifter till Finansinspektionen om den lägsta avgift som leverantören erbjuder alla konsumenter för de tjänster som framgår av den förteckning över de mest representativa tjänsterna knutna till betalkonton i Sverige som Finansinspektionen publicerar.

7 § Uppgifter enligt 6 § ska lämnas löpande via Finansinspektionens webbtjänst för löpande rapportering på det sätt som närmare anvisas där.

8 § Uppgifter enligt 6 § ska lämnas till Finansinspektionen senast samma bankdag som avgiften börjar tillämpas av betaltjänstleverantören.

Undantag från tillämpning i vissa fall

9 § Finansinspektionen kan besluta om undantag från bestämmelserna i 1, 2, 4 och 6 §§, om det finns särskilda skäl.

1. Dessa föreskrifter träder i kraft den 1 maj 2018, då Finansinspektionens föreskrifter (FFFS 2017:1) om vissa betalkonton ska upphöra att gälla.

2. Uppgifter enligt 6 kap. 2 § ska lämnas första gången senast den 21 augusti 2019 och avse perioden från och med den 1 januari 2019 till och med den 30 juni 2019.

ERIK THEDÉEN

David Lothigius