

## I

(Resolutioner, rekommendationer och yttranden)

## YTTRANDEN

## EUROPEISKA DATATILLSYNSMANNEN

**Yttrande från Europeiska datatillsynsmannen om kommissionens förslag till Europaparlamentets och rådets förordning om insiderhandel och otillbörlig marknadspåverkan samt till Europaparlamentets och rådets direktiv om straffrättsliga sanktioner för insiderhandel och otillbörlig marknadspåverkan**

(2012/C 177/01)

EUROPEISKA DATATILLSYNSMANNEN HAR AVGETT DETTA YTTRANDE

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artiklarna 7 och 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter <sup>(1)</sup>,

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter <sup>(2)</sup>, särskilt artikel 28.2.

HÄRIGENOM FRAMFÖRS FÖLJANDE:

## 1. INLEDNING

## 1.1 Samrådet med Europeiska datatillsynsmannen

1. Detta yttrande ingår i ett paket av fyra yttranden från Europeiska datatillsynsmannen om den finansiella sektorn som alla antogs samma dag <sup>(3)</sup>.
2. Den 20 oktober 2011 antog kommissionen ett förslag till Europaparlamentets och rådets förordning om insiderhandel och otillbörlig marknadspåverkan ("förslaget till förordning") och ett förslag till Europaparlamentets och rådets direktiv om straffrättsliga sanktioner för insiderhandel och otillbörlig marknadspåverkan ("förslaget till direktiv"). Förslaget till förordning och förslaget till direktiv (gemensamt kallade "förslagen") skickades av kommissionen till Europeiska datatillsynsmannen för samråd och mottogs den 31 oktober 2011. Den 6 december 2011 samrådde Europeiska unionens råd med Europeiska datatillsynsmannen om förslagen.

<sup>(1)</sup> EGT L 281, 23.11.1995, s. 31.

<sup>(2)</sup> EGT L 8, 12.1.2001, s. 1.

<sup>(3)</sup> Europeiska datatillsynsmannens yttranden av den 10 februari 2012 om lagstiftningspaketet om en översyn av banklagstiftningen, kreditratinginstituten, marknaderna för finansiella instrument (MIFID/MIFIR) och marknadsmissbruk.

3. Ett informellt samråd ägde rum med Europeiska datatillsynsmannen innan förslaget till förordning antogs. Europeiska datatillsynsmannen konstaterar att flera av hans kommentarer har beaktats i förslaget.
4. Europeiska datatillsynsmannen välkomnar samråden med kommissionens och rådet.

### 1.2 Förslagets syfte och omfattning

5. Genom direktivet om marknadsmissbruk <sup>(1)</sup> som antogs i början av 2003 infördes en gemensam ram inom EU för att förebygga, upptäcka och påföra sanktioner för såväl insiderhandel som otillbörlig marknadspåverkan.
6. När direktivet om marknadsmissbruk varit i kraft i flera år utvärderade kommissionen dess tillämpning och upptäckte ett antal problem, såsom luckor i regleringen av vissa instrument och marknader, brister i fråga om ett effektivt genomdrivande (tillsynsmyndigheterna saknar viss information och vissa befogenheter och sanktioner saknas eller är inte tillräckligt avskräckande), bristande klarhet i fråga om vissa nyckelbegrepp och administrativa bördor för emittenter.
7. Mot bakgrund av dessa problem och av de viktiga förändringar som genomförts av det finansiella landskapet genom utvecklingen på områden som lagstiftning, marknader och teknik, har kommissionen antagit förslag om ändring av direktivet om marknadsmissbruk som utgörs av förslaget till förordning och förslaget till direktiv. Det politiska syftet med förslagen är att öka investerarnas förtroende och marknadens integritet och att hålla jämna steg med utvecklingen inom den finansiella sektorn.
8. Genom framför allt förslaget till förordning utsträcks tillämpningsområdet för lagstiftningen om marknadsmissbruk, försök till otillbörlig marknadspåverkan och insiderhandel stämplas som separata brott, de behöriga myndigheternas befogenheter att genomföra utredningar stärks och minimiregler för administrativa åtgärder, sanktioner och böter införs.
9. Enligt förslaget till direktiv ska medlemsstaterna införa straffrättsliga påföljder för avsiktlig insiderhandel eller otillbörlig marknadspåverkan och för den som uppmuntrar, understödjer eller försöker begå något av de brotten. I förslaget till direktiv utsträcks även ansvarigheten, inklusive det straffrättsliga ansvaret, till juridiska personer i de fall där det är möjligt.

### 1.3 Syftet med Europeiska datatillsynsmannens yttrande

10. Flera av de åtgärder som planeras enligt förslagen för att uppnå ökad marknadsintegritet och ökat skydd för investerare har betydelse för enskilda personers rättigheter vad gäller behandlingen av deras personuppgifter.
11. När de behöriga myndigheterna undersöker eller samarbetar för att upptäcka, rapportera och/eller bestraffa insiderhandel eller otillbörlig marknadspåverkan kommer personuppgifter att samlas in, behandlas och utbytas. Mekanismerna för att uppmuntra personer att rapportera överträdelse kommer dessutom att medföra behandling av personuppgifter rörande såväl den person som rapporterar överträdelsen som den "anklagade" personen. Slutligen kommer sanktionssystemet att påverka rätten till skydd av personuppgifter eftersom sanktioner som röjer identiteten för den person som är skyldig till överträdelsen av den föreslagna förordningen kommer att offentliggöras.
12. Förslaget till förordning innehåller flera bestämmelser som kan påverka individens rätt till skydd av personuppgifter, medan förslaget till direktiv som sådant inte medför behandling av personuppgifter. Detta yttrande kommer därför i första hand att inriktas på förslaget till förordning och främst följande frågor: 1. dataskyddslagstiftningens tillämpbarhet, 2. insiderlistorna, 3. de behöriga myndigheternas befogenheter, 4. de system som finns för att upptäcka och rapportera misstänkta transaktioner, 5. utbytet av information med tredjeländer, 6. offentliggörandet av sanktioner och rapportering av överträdelse.

<sup>(1)</sup> Europaparlamentets och rådets direktiv 2003/6/EG av den 28 januari 2003 om insiderhandel och otillbörlig marknadspåverkan (marknadsmissbruk), EGT L 96, 12.4.2003, s. 16.

## 2. ANALYS AV FÖRSLAGEN

### 2.1 Dataskyddslagstiftningens tillämpbarhet

13. I såväl skälen <sup>(1)</sup> som bestämmelserna <sup>(2)</sup> i förslaget till förordning nämns stadgan om de grundläggande rättigheterna, direktiv 95/46/EG och förordning (EG) nr 45/2001. I artikel 22 i förslaget till förordning anges som en generell regel att "I fråga om medlemsstaternas behandling av personuppgifter inom ramen för denna förordning, ska behöriga myndigheter tillämpa bestämmelserna i direktiv 95/46/EG. I fråga om Esmas behandling av personuppgifter inom ramen för denna förordning, ska Esma följa bestämmelserna i förordning (EG) nr 45/2001." Enligt förordningen får dessutom personuppgifter bevaras i högst fem år.
14. Europeiska datatillsynsmannen välkomnar i hög grad denna övergripande bestämmelse och uppskattar den uppmärksamhet som ägnas frågorna om dataskydd i förslaget till förordning. Europeiska datatillsynsmannen föreslår emellertid att bestämmelsen omformuleras så att tillämpbarheten för den befintliga dataskyddslagstiftningen understryks. Hänvisningen till direktiv 95/46/EG bör dessutom förtydligas genom att det anges att bestämmelserna ska tillämpas i enlighet med de nationella bestämmelser som genomför direktiv 95/46/EG. Europeiska datatillsynsmannen konstaterar att vissa bestämmelser i förslaget till förordning uttryckligen hänvisar till direktiv 95/46/EG och/eller förordning (EG) nr 45/2001. Detta understryker tillämpningen av de relevanta dataskyddsreglerna i specifika fall, men det innebär inte att reglerna inte är tillämpbara när de inte uttryckligen nämns i varje bestämmelse som (eventuellt) skulle kunna innebära behandling av personuppgifter.
15. Precis som i skäl 33 bör även andra skäl konsekvent utformas så att medlemsstaterna "ska" och inte bara "bör" respektera den relevanta dataskyddslagstiftningen, eftersom den har trätt i kraft och det inte finns någon frihet att tillämpa den efter egen bedömning.

### 2.2 Insiderförteckningar

16. Enligt förslaget till förordning ska emittenter av ett finansiellt instrument eller deltagare på marknaden för utsläppshandel eller personer som handlar på deras vägnar eller för deras räkning upprätta en förteckning över alla personer som arbetar för dem, genom anställningskontrakt eller på annat vis, och som har tillgång till insiderinformation (artikel 13.1). Emittenter av ett finansiellt instrument vars finansiella instrument godkänts för handel på tillväxtmarknader för små och medelstora företag ska undantas från kravet på att upprätta en sådan lista om inte den behöriga myndigheten kräver en sådan lista (artikel 13.2).
17. Europeiska datatillsynsmannen inser behovet av sådana listor som ett viktigt redskap för de behöriga myndigheterna när de undersöker eventuell insiderhandel eller otillbörlig marknadspåverkan. I den utsträckning som dessa listor innebär behandling av personuppgifter bör emellertid centrala regler och garantier för dataskydd anges i grundlagstiftningen. Europeiska datatillsynsmannen rekommenderar därför att det görs en uttrycklig hänvisning till syftet med en sådan lista i en materiell bestämmelse i förslaget till förordning. Syftet är i själva verket ett av de viktigaste inslagen i all databehandling enligt artikel 6 i direktiv 95/46/EG.
18. Enligt artikel 13.4 i förslaget till förordning ska kommissionen, genom delegerade akter, anta åtgärder som fastställer innehållet i en sådan lista, inklusive dels information om identiteten på personerna på listan och skälen till varför de förts upp på den, dels villkoren för hur emittenter av finansiella instrument eller deltagare på marknaden för utsläppshandel, eller enheter som handlar på deras vägnar, ska upprätta en sådan lista, villkoren för uppdatering av listor samt hur länge de ska bevaras och ansvarsområdena för personerna på listan. Datatillsynsmannen rekommenderar emellertid följande:
- De viktigaste inslagen i listan (under alla omständigheter skälen till att personer tas med) bör anges i förslaget till förordning.
  - Det bör införas en hänvisning till behovet av att samråda med Europeiska datatillsynsmannen om delegerade akter som avser behandlingen av personuppgifter.

### 2.3 De behöriga myndigheternas befogenheter

19. I artikel 17.2 anges de tillsyns- och övervakningsbefogenheter som de behöriga myndigheterna minst bör ha för att utföra sina uppgifter enligt förslaget till förordning.

<sup>(1)</sup> Se skälen 33, 35, 39 och 40 i förslaget till förordning.

<sup>(2)</sup> Se artiklarna 17.4, 22, 23 och 29.1 c i förslaget till förordning.

20. Två befogenheter behöver uppmärksammas särskilt eftersom de strider mot rätten till personlig integritet och dataskydd: Rätten att gå in i privatbostäder för att lägga beslag på dokument, oavsett typ, och rätten att begära in befintliga uppgifter över tele- och datatrafik.

### 2.3.1 Rätten att gå in i privatbostäder

21. Rätten att gå in i privatbostäder för att lägga beslag på dokument, oavsett typ, innebär ett kraftigt intrång i privatlivet och strider mot rätten till personlig integritet. Den bör därför omfattas av strikta villkor och omges av adekvata skyddsåtgärder<sup>(1)</sup>. Enligt artikel 17.2 e ska det krävas förhandsgodkännande från den berörda medlemsstatens rättsliga myndighet i enlighet med nationell lag och en rimlig misstanke om att det finns dokument med koppling till kontrollen som kan vara relevanta för att bevisa att det föreligger insiderhandel eller otillbörlig marknadspåverkan för att gå in i privatbostäder. Europeiska datatillsynsmannen uppskattar att texten inskränker de behöriga myndigheternas befogenheter genom att kräva att det ska föreligga en rimlig misstanke om överträdelse av den föreslagna förordningen eller direktivet och ett förhandsgodkännande från en rättslig myndighet som villkor för att gå in i privatbostäder. Europeiska datatillsynsmannen anser emellertid att ett generellt krav på förhandsgodkännande från rättsliga myndigheter, oavsett om detta krävs i den nationella lagstiftningen eller ej, är såväl motiverat som nödvändigt med tanke på det potentiella intrång som den aktuella befogenheten kan innebära.

22. I skäl 30 till förslaget till förordning anges de fall där tillträde till privatbostäder är nödvändigt, dvs. i synnerhet om den person som redan har mottagit en begäran om information (helt eller delvis) underlåter att hörsamma den, eller om det finns rimliga skäl att anta att en eventuell begäran inte skulle höras eller att de dokument eller upplysningar som informationskravet avser skulle undanröjas, manipuleras eller förstöras. Europeiska datatillsynsmannen välkomnar dessa preciseringar. Han anser emellertid att det krävs ytterligare skyddsåtgärder för att garantera respekten för rätten till personlig integritet och att sådana därför bör införas i en materiell bestämmelse som ett villkor för att gå in i privatbostäder.

### 2.3.2 Befogenheten att begära in befintliga uppgifter över tele- och datatrafik

23. Enligt artikel 17.2 f ska de behöriga myndigheterna ha rätt att "[b]egära in befintliga uppgifter över tele- och datatrafik som innehas av en teleoperatör eller ett värdepappersföretag", men det förtydligas att det måste föreligga en "rimlig misstanke" om att sådana uppgifter "kan vara av betydelse för att bevisa insiderhandel eller otillbörlig marknadspåverkan" enligt definitionen i förslaget till förordning eller förslaget till direktiv. De uppgifterna ska dock inte röra "innehållet i det meddelande de berör". Enligt artikel 17.3 ska dessutom de befogenheter som anges i artikel 17.2 utövas i enlighet med nationell lag.

24. Uppgifter i samband med användningen av elektroniska kommunikationsmetoder kan förmedla en mängd personlig information, till exempel identiteten för de personer som gör och tar emot samtalet, samtalets tidpunkt och varaktighet, vilket nät som använts, användarens geografiska placering om det handlar om mobiltelefoner etc. Vissa trafikdata som avser internet- och e-postanvändning (till exempel listan över besökta webbplatser) kan dessutom avslöja viktiga uppgifter om innehållet i kommunikationen. Behandling av trafikuppgifter strider dessutom mot brevsekretessen. I samband med detta har principen att trafikuppgifter måste raderas eller göras anonyma när de inte längre behövs för att skicka ett meddelande fastställts i direktiv 2002/58/EG<sup>(2)</sup> (direktivet om integritet och elektronisk kommunikation)<sup>(3)</sup>. Enligt artikel 15.1 i det direktivet får medlemsstaterna införa undantag i den nationella lagstiftningen för vissa specifika legitima syften när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att uppnå sådana syften<sup>(4)</sup>.

<sup>(1)</sup> Se framför allt Europadomstolen, 23 februari 1993, *Funcke mot Frankrike*, 10828/84.

<sup>(2)</sup> Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

<sup>(3)</sup> Se artikel 6.1 i direktiv 2002/58/EG (EGT L 201, 31.7.2002, s. 45).

<sup>(4)</sup> Enligt artikel 15.1 i direktiv 2002/58/EG får medlemsstaterna vidta sådana åtgärder "när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i direktiv 95/46/EG. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som fastställs i denna punkt (...)"

25. Europeiska datatillsynsmannen inser att de syften som kommissionen vill uppnå med förslaget till förordning är legitima. Han inser behovet av initiativ som stärker övervakningen av finansmarknaderna för att de ska förbli sunda och för att bättre skydda investerare och ekonomin i stort. Undersökningsbefogenheter som direkt avser trafikdata måste uppfylla kraven på nödvändighet och proportionalitet, dvs. de måste vara begränsade till vad som är lämpligt för att uppnå målet eftersom de befogenheterna innebär ett kraftigt intrång<sup>(1)</sup>. Det är därför viktigt mot den bakgrunden att bestämmelserna utformas tydligt när det gäller deras personliga och materiella omfattning samt de omständigheter och villkor enligt vilka de kan användas. Dessutom måste tillräckliga säkerhetsåtgärder införas mot risken för missbruk.
26. Uppgifter om telefon- och datatrafik kommer självklart att omfatta personuppgifter i den mening som anges i direktiv 95/46/EG, direktiv 2002/58/EG och förordning (EG) nr 45/2001. I skäl 31 i förslaget till förordning framhålls följande: "Uppgifter om tele- och datatrafik kan göra det möjligt att fastställa identiteten på en person som ansvarar för spridningen av falsk eller vilseledande information, fastställa att personer varit i kontakt med varandra en viss tidpunkt och fastställa att det finns en koppling mellan två eller fler personer"<sup>(2)</sup>. Man måste därför se till att villkoren för en rättvis och lagenlig behandling av personuppgifter, på det vis som anges i direktiven och förordningen, respekteras fullt ut.

### 2.3.3 Kravet på rättsligt förhandsgodkännande

27. Europeiska datatillsynsmannen konstaterar att enligt artikel 17.3 ska denna befogenhet utövas i enlighet med nationell lagstiftning utan att det uttryckligen hänvisas till ett rättsligt förhandsgodkännande, som var fallet när det gällde befogenheten att gå in i privatbostäder. Europeiska datatillsynsmannen anser att ett generellt krav på rättsligt förhandsgodkännande i samtliga fall – oavsett om det krävs i den nationella lagstiftningen eller ej – skulle vara motiverat eftersom den aktuella befogenheten kan innebära ett kraftigt intrång och för att lagen ska tillämpas enhetligt i alla EU:s medlemsstater. Man bör också beakta att olika lagar i medlemsstaterna har särskilda garantier för hemmets okränkbarhet gentemot oproportionella och inte omsorgsfullt reglerade inspektioner, undersökningar eller beslagtaganden, framför allt när de utförs av administrativa institutioner.
28. Europeiska datatillsynsmannen rekommenderar dessutom att det införs ett krav för de behöriga myndigheterna att begära in uppgifter om telefon- och datatrafik genom formella beslut som anger den rättsliga grunden och syftet med begäran och vilken information som krävs, den tidsfrist inom vilken information ska lämnas samt den berörda personens rätt att få beslutet granskat av domstolen.

### 2.3.4 Definition av telefon- och datatrafikuppgifter

29. Det finns ingen definition av begreppen "uppgifter om telefon- och datatrafik" i förslaget till förordning. I direktiv 2002/58/EG (om elektronisk kommunikation) hänvisas enbart till "trafikuppgifter", men inte till "uppgifter över telefon- och datatrafik". Självklart kommer den exakta innebörden av dessa begrepp att bestämma vilken effekt undersökningsbefogenheterna kan få för de berörda personernas integritet och dataskydd. Europeiska datatillsynsmannen föreslår att man använder den terminologi som redan finns i definitionen av "trafikuppgifter" i direktiv 2002/58/EG.
30. I artikel 17.2 f hänvisas till "befintliga uppgifter över tele- och datatrafik som innehas av en teleoperatör". I direktivet om elektronisk kommunikation fastställs principen att alla trafikuppgifter måste raderas när de inte längre behövs för det kommersiella syfte för vilket de samlades in. På grundval av artikel 15.1 i direktivet om elektronisk kommunikation kan emellertid medlemsstaterna göra undantag från denna skyldighet av skäl som rör rättssäkerheten. Syftet med direktivet om datalagring är att anpassa medlemsstaternas initiativ enligt artikel 15.1 i direktivet om elektronisk kommunikation vad gäller bevarande av uppgifter för utredning, upptäckande och lagföring av "allvarliga" brott.

<sup>(1)</sup> Se t.ex. de förenade målen C-92/09 och C-93/09, *Volker und Markus Schecke GbR (C-92/09)*, *Hartmut Eifert (C-92/09)* v. *Land Hessen*, ännu inte offentliggjorda i REU, punkt 74.

<sup>(2)</sup> Se också s. 12 i motiveringen till förslaget till förordning.

31. Frågan är om de uppgifter om telefon- och datatrafik som anges i artikel 17.2 f avser sådana uppgifter som är tillgängliga genom bevarande av trafik- och lokaliseringsdata som regleras i direktivet om elektronisk kommunikation eller de ytterligare uppgifter som krävs enligt direktivet om datalagring. Det senare alternativet skulle skapa allvarliga problem, eftersom undantagen som anges i artikel 15.1 i direktivet om elektronisk kommunikation (dvs. förebyggande, undersökning, avslöjande av och åtal för brott) skulle användas för att bredda de syften för vilka uppgifter bevaras enligt direktivet om datalagring (dvs. undersökning och avslöjande av och åtal för "allvarliga" brott). De uppgifter som lagras enligt direktivet om datalagring skulle med andra ord användas för syften som inte anges i det direktivet. Det skulle innebära att EU stöder att man utnyttjar den "lucka i lagen" som är en av de viktigaste bristerna i det nuvarande direktivet om datalagring <sup>(1)</sup>.
32. Europeiska datatillsynsmannen rekommenderar därför kraftigt att man specificerar de typer av uppgifter om telefon- och datatrafik som de behöriga myndigheterna kan begära in. Sådana uppgifter måste vara adekvata, relevanta och inte överdrivna i förhållande till det syfte för vilka de begärs in och behandlas. Europeiska datatillsynsmannen rekommenderar dessutom att artikel 17.2 f begränsas till uppgifter som normalt behandlas ("innehåser") av telekommunikationsoperatörer inom ramen för direktivet om elektronisk kommunikation 2002/58/EG. Detta utesluter i princip tillgång till uppgifter som förvaras för de syften som anges i direktivet om datalagring, eftersom sådan tillgång inte begärs i syfte att undersöka, avslöja och åtala för "allvarliga" brott <sup>(2)</sup>.
33. Enligt artikel 17.2 f beviljas tillgång till "uppgifter över tele- och datatrafik som innehåses av [...] ett värdepappersföretag". I texten bör typerna av uppgifter specificeras och det bör förtydligas vilka företag som bestämmelsen avser. Europeiska datatillsynsmannen antar att uppgifterna kommer att sammanfalla med dem som anges i förslaget till Europaparlamentets och rådets direktiv om marknader för finansiella instrument ("förslaget till MiFID"). Han understryker att han lämnade vissa synpunkter på det förslaget och rekommenderade att även dessa begrepp förtydligas <sup>(3)</sup>. Eftersom uppgifterna om telefon- och trafikdata skulle gälla de telefonkonversationer och den elektroniska kommunikation som anges i artikel 16.7 i förslaget till MiFID rekommenderade Europeiska datatillsynsmannen att syftet med att registrera sådana kommunikationer definieras och att typen av kommunikation anges, liksom vilka kategorier av data från kommunikationerna som registreras <sup>(4)</sup>.
34. Europeiska datatillsynsmannen gläder sig slutligen åt att det enligt texten krävs en rimlig misstanke om överträdelse av förslaget till förordning eller förslaget till direktiv för att de behöriga myndigheterna ska få tillgång till uppgifterna och att deras tillgång till meddelandenas innehåll uttryckligen undantas.

#### 2.4 System för att upptäcka och rapportera misstänkta transaktioner

35. I artikel 11.1 i förslaget till förordning föreskrivs att alla personer som driver en handelsplats ska anta och underhålla effektiva system och förfaranden i syfte att förhindra och upptäcka otillbörlig marknadspåverkan. I artikel 11.2 föreskrivs vidare att personer som yrkesmässigt arrangerar eller genomför transaktioner med finansiella instrument ska ha infört system som upptäcker och rapporterar handelsorder och transaktioner som kan utgöra insiderhandel, otillbörlig marknadspåverkan eller försök till

<sup>(1)</sup> Se i detta sammanhang Europeiska datatillsynsmannens yttrande av den 31 maj 2011 om kommissionens utvärderingsrapport till rådet och Europaparlamentet om direktivet om datalagring (direktiv 2006/24/EG), t.ex. punkt 24.

<sup>(2)</sup> Europeiska datatillsynsmannen vill påminna om problemen i samband med bristen på en europeisk definition av "allvarliga brott". Europeiska datatillsynsmannen underströk i själva verket att kommissionens utvärderingsrapport om direktivet om datalagring visar att valet att överlämna definitionen av vad som utgör "allvarliga brott" till medlemsstaternas bedömning har lett till att uppgifterna har använts för ett stort antal olika syften. Enligt kommissionen medger de flesta av medlemsstaterna som genomfört direktivet i enlighet med den egna lagstiftningen tillgång till och användning av lagrade uppgifter för syften som går utöver dem som omfattas av direktivet, inklusive att förhindra och bekämpa brottslighet i allmänhet och minska risken för liv och hälsa. Se yttrande av den 31 maj 2011 om kommissionens utvärderingsrapport till rådet och Europaparlamentet om direktivet om datalagring (direktiv 2006/24/EG), punkterna 24, 71 och 72.

<sup>(3)</sup> Enligt artikel 71.2 d har de behöriga myndigheterna enligt förslaget till MiFID rätt att begära in befintliga uppgifter över telefon- och datatrafik som innehåses av värdepappersföretag om det finns en rimlig misstanke om brott mot bestämmelserna i förslaget till MiFID.

<sup>(4)</sup> Se Europeiska datatillsynsmannens yttrande av den 10 februari om förslaget till Europaparlamentets och rådets direktiv om marknader för finansiella instrument och om upphävande av Europaparlamentets och rådets (omarbetade) direktiv 2004/39/EG och till Europaparlamentets och rådets förordning om marknader för finansiella instrument och om ändring av förordning [EMIR] om OTC-derivat, centrala motparter och transaktionsregister.

sådan marknadspåverkan eller insiderhandel. Om det föreligger misstankar ska den behöriga myndigheten omedelbart underrättas. Kommissionen ska anta tekniska standarder för tillsyn för att fastställa de lämpliga system och förfaranden som avses i punkt 1 och de system och mallar för anmälan som avses i punkt 2 (artikel 11.3 sista meningen).

36. Eftersom dessa system högst sannolikt kommer att behandla personuppgifter (t.ex. övervakning av transaktioner som görs av personer som är upptagna på insiderförteckningar), vill Europeiska datatillsynsmannen understryka att standarderna bör utvecklas enligt principen om "inbyggt integritetsskydd", dvs. att uppgiftsskydd och integritet införlivas redan vid framtagningen av nya produkter, tjänster och förfaranden som omfattar behandling av personuppgifter<sup>(1)</sup>. Dessutom rekommenderar Europeiska datatillsynsmannen att man infogar att Europeiska datatillsynsmannen måste rådfrågas om dessa regleringsstandarder berör behandling av personuppgifter.

## 2.5 Informationsutbyte med tredjeländer

37. Europeiska datatillsynsmannen noterar hänvisningen till direktiv 95/46/EG, särskilt till artikel 25 eller 26, och de särskilda skyddsmekanismerna i artikel 23 i förslaget till förordning angående överföring av personuppgifter till tredjeland. I synnerhet bedömningen från fall till fall, fastställandet att överföringen är nödvändig, kravet på uttryckligt godkännande i förväg från den behöriga myndigheten av ytterligare överföring av uppgifter till och av ett tredjeland samt att det finns en tillräckligt hög skyddsnivå för personuppgifter i det tredjeland som tar emot personuppgifterna anses vara lämpliga skyddsmekanismer med hänsyn till riskerna med sådana överföringar.

## 2.6 Offentliggörande av påföljder

### 2.6.1 Obligatoriskt offentliggörande av påföljder

38. I artikel 26.3 i förslaget till förordning åläggs medlemsstaterna att se till att de behöriga myndigheterna utan onödigt dröjsmål offentliggör alla administrativa åtgärder och påföljder som utfärdats för överträdelser av den föreslagna förordningen. Offentliggörandet ska minst innehålla vilken typ av överträdelse det rör sig om och vilka som begått den, om offentliggörandet inte innebär ett allvarligt hot mot stabiliteten på de finansiella marknaderna.
39. Offentliggörandet av påföljder bör kunna bidra till att öka systemets avskräckande effekt genom att de som verkligen begår eller kan komma att begå överträdelser avhåller sig från detta för att undvika att deras renommé försämras betydligt. Det skulle dessutom öka öppenheten eftersom marknadsaktörerna blir uppmärksammade på att en viss person begått en överträdelse. Denna skyldighet inskränks endast om offentliggörandet skulle orsaka oproportionell skada för de berörda parterna, då de behöriga myndigheterna ska offentliggöra påföljderna på anonym grund.
40. Europeiska datatillsynsmannen välkomnar hänvisningen till Europeiska unionens stadga om de grundläggande rättigheterna i skäl 35 och i synnerhet till rätten till skydd av personuppgifter vid antagandet och offentliggörandet av påföljder. Han är dock inte övertygad om att det obligatoriska offentliggörandet av påföljder, så som kravet nu är formulerat, uppfyller kraven i lagstiftningen om uppgiftsskydd i överensstämmelse med domstolens rättspraxis i Schecke-målet<sup>(2)</sup>. Han anser att ändamålet, nödvändigheten och proportionaliteten hos åtgärden inte är tillräckligt klargjorda och att ändamålsenliga skyddsmekanismer under alla omständigheter borde ha föreskrivits för att inte äventyra den enskildes rättigheter.

### 2.6.2 Offentliggörandets nödvändighet och proportionalitet

41. I Schecke-målet ogiltigförklarade domstolen bestämmelserna i rådets och kommissionens förordning om obligatoriskt offentliggörande av uppgifter om mottagare av stöd från jordbruksfonderna, inklusive mottagarens namn och de mottagna beloppen. Domstolen ansåg att offentliggörandet utgjorde behandling av personuppgifter som omfattas av artikel 8.2 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och därför innebar ett ingrepp i rättigheterna enligt artiklarna 7 och 8 i den stadgan.

<sup>(1)</sup> Se Europeiska datatillsynsmannens yttrande av den 14 januari 2011 om kommissionens meddelande till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén – "Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen", (EUT C 181, 22.6.2011, s. 1), punkterna 108–115.

<sup>(2)</sup> Förenade målen C-92/09 och C-93/09, Schecke, punkterna 56–64.

42. Efter att ha konstaterat att "undantag och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är absolut nödvändigt", prövade domstolen ändamålet med och proportionaliteten hos offentliggörandet. Domstolen fann att ingenting tydde på att rådet och kommissionen när de antog den berörda lagstiftningen hade övervägt andra metoder att offentliggöra uppgifterna som är förenliga med det mål som eftersträvas med offentliggörandet men som ändå innebär ett mindre långtgående ingrepp i stödmottagarnas rättigheter.
43. Artikel 26.3 i förslaget till förordning tycks lida av samma brister som domstolen framhöll i Scheckemålet. När det gäller bedömningen av om en bestämmelse om offentliggörande av personuppgifter är förenlig med kravet på uppgiftsskydd erinrar Europeiska datatillsynsmannen om vikten av att ha ett tydligt och väldefinierat ändamål för offentliggörandet. Det är endast med ett tydligt och väldefinierat ändamål som det går att bedöma om det verkligen är nödvändigt och står i proportion till målet att offentliggöra de berörda personuppgifterna <sup>(1)</sup>.
44. Efter att ha läst förslaget och de åtföljande dokumenten (dvs. konsekvensanalysen) har Europeiska datatillsynsmannen intrycket att åtgärdens ändamål, och följaktligen dess nödvändighet, inte är tydligt fastslagen. I skälen till förslaget nämns inte dessa frågor och i konsekvensanalysen hänvisas det endast till allmänna konsekvenser (dvs. till den avskräckande effekten i fråga om marknadsmissbruk, bidraget till investerarskyddet, lika behandling av emittenter, förbättrad efterlevnad) och det nämns endast att "offentliggörandet av påföljder är mycket viktigt för att förbättra öppenheten och bevara förtroendet för finansmarknaden" och att "offentliggörandet av vidtagna sanktionsåtgärder kommer att bidra till målet att avskräcka från överträdelse och förbättra marknadens integritet och investerarskyddet" <sup>(2)</sup>. Ett så allmänt påstående verkar inte räcka för att visa att den föreslagna åtgärden är nödvändig. Om det allmänna målet är att öka den avskräckande effekten, borde kommissionen i synnerhet ha förklarat varför det inte skulle ha räckt med kraftigare ekonomiska sanktioner (eller andra sanktioner än sådana som går ut på "uthängning").
45. Vidare tycks man i konsekvensanalysen inte ha beaktat mindre ingripande metoder, exempelvis att offentliggörandet ska beslutas från fall till fall. I synnerhet det senare alternativet ser vid första anblicken ut att vara en lösning som står mer i proportion till målet, särskilt om man betänker att offentliggörandet är en påföljd – vilket erkänns i artikel 26.1 d – och som därför ska bedömas från fall till fall med beaktande av de berörda omständigheterna, bland annat hur allvarlig överträdelsen är, graden av personligt ansvar, återfall, förluster för tredje part m.m. <sup>(3)</sup>
46. I konsekvensanalysen förklaras inte varför offentliggörandet efter en bedömning från fall till fall inte är ett tillräckligt alternativ. Det nämns endast att offentliggörandet av fastställandet av påföljder "bidrar till målet att om möjligt eliminera alternativ och handlingsutrymmen genom att avskaffa den rätt som medlemsstaterna för närvarande har att inte kräva ett sådant offentliggörande" <sup>(4)</sup>. Enligt Europeiska datatillsynsmannens mening står möjligheten att bedöma ett fall med hänsyn till de särskilda omständigheterna mer i proportion till målet och är därför ett alternativ som bör föredras framför obligatoriskt offentliggörande i samtliga fall. Denna handlingsfrihet skulle exempelvis göra det möjligt för de behöriga myndigheterna att avstå från att offentliggöra mindre allvarliga överträdelse, om överträdelsen inte orsakat betydande skada, om den berörda parten har visat sig vara samarbetsvillig m.m. Bedömningen i konsekvensanalysen skingrar därför inte tvivlen om att åtgärden är nödvändig och proportionell.

### 2.6.3 Behovet av ändamålsenliga skyddsmekanismer

47. I förslaget till förordning borde man ha föreskrivit ändamålsenliga skyddsmekanismer för att få en rimlig balans mellan de olika berörda intressena. För det första är skyddsmekanismer nödvändiga för de anklagade personernas rätt att få ett beslut prövat inför domstol och åtnjuta oskuldspresumtion. En

<sup>(1)</sup> Se även i detta sammanhang Europeiska datatillsynsmannens yttrande av den 15 april 2011 om finansiella bestämmelser för unionens årliga budget (EUT C 215, 21.7.2011, s. 13).

<sup>(2)</sup> Se konsekvensanalysen s. 166.

<sup>(3)</sup> Det vill säga i enlighet med artikel 27 i förslaget till förordning där det föreskrivs kriterier för fastställandet av påföljder.

<sup>(4)</sup> Se konsekvensanalysen, s. 167.



uttrycklig bestämmelse om detta borde ha ingått i texten i artikel 26.3 så att de behöriga myndigheterna blir skyldiga att vidta tillräckliga åtgärder både i de fall då ett beslut har överklagats och i de fall då beslutet slutligen ogiltigförklaras av en domstol <sup>(1)</sup>.

48. För det andra bör man i förslaget till förordning se till att de berörda rättigheter respekteras på ett förutseende sätt. Europeiska datatillsynsmannen skulle uppskatta att man i den slutliga versionen av förslaget föreskriver en möjlighet att avstå från offentliggörande i de fall då det skulle orsaka oproportionell skada. Ett förutseende tillvägagångssätt borde också innebära att de berörda personerna informeras i förväg om att beslutet att fastställa påföljder mot dem kommer att offentliggöras och att de i enlighet med artikel 14 i direktiv 95/46/EG har rätt att invända mot detta om det finns avgörande och berättigade skäl <sup>(2)</sup>.
49. För det tredje anges det inte i förslaget till förordning i vilket medium uppgifterna ska offentliggöras. Man kan tänka sig att offentliggörandet i praktiken kommer att ske på internet i de flesta medlemsstater. Offentliggörande på internet väcker särskilda frågor och farhågor, framför allt man måste se till att informationen inte finns kvar på nätet längre än nödvändigt och att uppgifterna inte kan manipuleras eller ändras. Användningen av externa sökmotorer medför också risken att informationen tas ur sitt sammanhang och distribueras både via webben och utanför på ett sätt som är svårt att kontrollera <sup>(3)</sup>.
50. Med hänsyn till ovanstående är det nödvändigt att ålägga medlemsstaterna att se till att personuppgifter om de berörda personerna finns kvar på nätet endast under en rimlig tidsperiod, varefter de systematiskt ska utplånas <sup>(4)</sup>. Medlemsstaterna bör också vara skyldiga att se till att det finns ändamålsenliga säkerhetsåtgärder och skyddsmekanismer, särskilt för att skydda mot risken att uppgifterna används av externa sökmotorer <sup>(5)</sup>.

#### 2.6.4 Slutsatser

51. Europeiska datatillsynsmannen anser att bestämmelsen om obligatoriskt offentliggörande av påföljder – så som den nu är formulerad – inte är förenlig med den grundläggande rätten till personlig integritet och skydd av personuppgifter. Lagstiftaren bör noga överväga om det föreslagna systemet är nödvändigt och kontrollera om kravet på offentliggörande går utöver vad som är nödvändigt för att uppnå det eftersträvade allmännyttiga ändamålet och om det finns mindre ingripande sätt att uppnå samma mål. Beroende av resultaten av denna proportionalitetsprövning bör kravet på offentliggörande under alla omständigheter stödjas av ändamålsenliga skyddsmekanismer för att se till att oskuldspresumtionen respekteras liksom de berörda personernas rätt att invända, uppgifternas säkerhet och riktighet samt att uppgifterna utplånas efter en lämplig tidsperiod.

### 2.7 Rapportering av överträdelser

52. Enligt artikel 29 i förslaget till förordning ska medlemsstaterna införa effektiva mekanismer för att slå larm om och rapportera missförhållanden ("whistle-blowing"). Detta kan visserligen fungera som ett effektivt medel för efterlevnad men sådana system väcker betydande farhågor ur ett uppgiftsskydds-perspektiv <sup>(6)</sup>.

<sup>(1)</sup> Exempelvis borde de nationella myndigheterna överväga följande åtgärder: att skjuta upp offentliggörandet tills överklagandet ogillats eller, så som föreslås i konsekvensanalysen, tydligt ange att beslutet fortfarande kan överklagas och att den berörda personen betraktas som oskyldig till beslutet vunnit laga kraft, och offentliggöra en rättelse i de fall då ett beslut har upphävts av en domstol.

<sup>(2)</sup> Se Europeiska datatillsynsmannens yttrande av den 10 april 2007 om finansieringen av den gemensamma jordbrukspolitiken, (EUT C 134, 16.6.2007, s. 1).

<sup>(3)</sup> Se i detta sammanhang det dokument som offentliggjorts av den italienska dataskyddsmyndigheten, "Personal Data As Also Contained in Records and Documents by Public Administrative Bodies: Guidelines for Their Processing by Public Bodies in Connection with Web-Based Communication and Dissemination", som finns tillgängligt på den italienska dataskyddsmyndighetens webbplats, <http://www.garanteprivacy.it/garante/doc.jsp?ID=1803707>

<sup>(4)</sup> Dessa farhågor gäller också den mer allmänna rätten att bli bortglömd, vars införande i det nya regelverket för skydd av personuppgifter är under diskussion.

<sup>(5)</sup> Dessa åtgärder och skyddsmekanismer kan till exempel bestå av att utesluta informationen från dataindexering genom externa sökmotorer.

<sup>(6)</sup> Arbetsgruppen för skydd av uppgifter (nedan kallad *artikel 29-gruppen*) offentliggjorde 2006 ett yttrande om sådana system där uppgiftsskyddsaspekter av företeelsen togs upp: Artikel 29-gruppens yttrande nr 1/2006 om tillämpningen av EU:s dataskyddsregler på interna system för anmälan av missförhållanden när det gäller räkenskaper, intern granskning av räkenskaper, revision, bekämpning av mutor, bankväsende och finansiell brottslighet. Yttrandet finns på artikel 29-gruppens webbplats: [http://ec.europa.eu/justice/policies/privacy/workinggroup/index\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm)

53. Europeiska datatillsynsmannen välkomnar att förslaget till förordning innehåller särskilda skyddsmekanismer, som ska utvecklas vidare på nationell nivå, för att skydda personer som rapporterar misstänkta överträdelse och mer allmänt för skydd av personuppgifter. Europeiska datatillsynsmannen är medveten om att man i förslaget till förordning endast anger de viktigaste punkterna i det system som medlemsstaterna ska införa. Han vill ändå rikta uppmärksamheten på följande ytterligare punkter.
54. Precis som i andra yttranden framhåller Europeiska datatillsynsmannen <sup>(1)</sup> att det behöver införas en särskild bestämmelse om behovet av att skydda uppgiftslämnarnas identitet. Europeiska datatillsynsmannen vill betona att uppgiftslämnare befinner sig i en utsatt position. Personer som lämnar sådan information bör få garantier om att deras identitet hemlighålls, särskilt för den person som påstås vara ansvarig för den överträdelse som rapporteras <sup>(2)</sup>. Hemlighållandet av en uppgiftslämnarens identitet måste garanteras i alla etapper av förfarandet så länge som detta inte strider mot nationella bestämmelser för rättsliga förfaranden. I synnerhet kan identiteten behöva lämnas ut i samband med ytterligare utredningar eller senare rättsliga förfaranden som inleds till följd av utredningen (bland annat om det har fastställts att uppgiftslämnarna av illvilja har lämnat oriktiga uppgifter om den anklagade) <sup>(3)</sup>. Med hänsyn till ovanstående rekommenderar Europeiska datatillsynsmannen att följande bestämmelse läggs till i artikel 29.1 b: "Hemlighållandet av dessa personers identitet måste garanteras i alla etapper av förfarandet, såvida inte nationell lag kräver att deras identitet lämnas ut i samband med ytterligare utredning eller senare rättsliga förfaranden".
55. Europeiska datatillsynsmannen välkomnar att medlemsstaterna i artikel 29.1 c åläggs att säkerställa skyddet av personuppgifter både för den person som rapporterar överträdelse och för den anklagade personen i enlighet med principerna i direktiv 95/46/EG. Han föreslår dock att "principerna i" stryks för att göra hänvisningen till direktivet mer allmängiltig och bindande. När det gäller behovet av att respektera lagstiftningen om uppgiftsskydd i det praktiska genomförandet av systemen vill Europeiska datatillsynsmannen särskilt understryka de rekommendationer som artikel 29-gruppen lämnade i sitt yttrande 2006 om system för anmälan av missförhållanden. Vid genomförandet av de nationella systemen bör de berörda enheterna framför allt respektera proportionaliteten genom att så långt möjligt begränsa de kategorier av personer som har rätt att rapportera, de kategorier av personer som kan anklagas och de överträdelse som dessa kan anklagas för, behovet av att främja identifierade och konfidentiella rapporter framför anonyma rapporter, behovet av att kunna avslöja uppgiftslämnarens identitet om uppgiftslämnaren lämnat oriktiga uppgifter av illvilja samt behovet av att iakttä strikta tidsfrister för bevarande av uppgifter.

### 3. SLUTSATSER

56. Europeiska datatillsynsmannen välkomnar den särskilda uppmärksamhet som ägnats åt uppgiftsskydd i förslaget till förordning.
57. Europeiska datatillsynsmannen lämnar följande rekommendationer:
- Ange ändamålet med insiderförteckningen i artikel 13.
  - Inför förhandsgodkännande av domstol som ett allmänt krav i artikel 17.2 e om befogenheten att gå in i privatbostäder.
  - Inför förhandsgodkännande av domstol som ett allmänt krav i artikel 17.2 f om befogenheten att begära in uppgifter om tele- och datatrafik samt krav på ett formellt beslut där man specificerar i) den rättsliga grunden, ii) syftet med begäran, iii) vilken information som krävs, iv) tidsgränsen inom vilken informationen ska tillhandahållas samt v) mottagarens rätt att få beslutet granskat av EU-domstolen.

<sup>(1)</sup> Se exempelvis Europeiska datatillsynsmannens yttrande av den 15 april 2011 om finansiella bestämmelser för unionens årliga budget och yttrandet av den 1 juni 2011 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf), som båda är tillgängliga på <http://www.edps.europa.eu>

<sup>(2)</sup> Vikten av att hemlighålla uppgiftslämnarens identitet har redan betonats av Europeiska datatillsynsmannen i en skrivelse till Europeiska ombudsmannen av den 30 juli 2010 i ärende 2010-0458, som finns på Europeiska datatillsynsmannens webbplats (<http://www.edps.europa.eu>). Se även Europeiska datatillsynsmannens tidigare yttranden om förhandsgranskning av den 3 februari 2012 och av den 23 juni 2006 om Olafs interna utredningar (ärende 2005-0418) samt av den 4 oktober 2007 om Olafs externa utredningar (ärendena 2007-47, 2007-48, 2007-49, 2007-50, 2007-72).

<sup>(3)</sup> Se Europeiska datatillsynsmannens yttrande av den 15 april 2011 om finansiella bestämmelser för unionens årliga budget, som finns på datatillsynsmannens webbplats: <http://www.edps.europa.eu>

- Specificera de kategorier av telefon- och datatrafikuppgifter som innehas av teleoperatörer eller värdepappersföretag som de behöriga myndigheterna kan kräva in och begränsa artikel 17.2 f till uppgifter som normalt behandlas ("innehas") av teleoperatörer inom ramen för direktiv 2002/58/EG.
- Lägga till en bestämmelse i artikel 29.1 b: "Hemlighållandet av dessa personers identitet måste garanteras i alla etapper av förfarandet, såvida inte nationell lag kräver att deras identitet lämnas ut i samband med ytterligare utredning eller senare rättsliga förfaranden."
- Utvärdera nödvändigheten och proportionaliteten i det föreslagna systemet för obligatoriskt offentliggörande av påföljder mot bakgrund av de farhågor som framförts i detta yttrande. Beroende av resultaten av denna proportionalitetsprövning bör man under alla omständigheter sörja för ändamålsenliga skyddsmekanismer för att se till att oskuldspresumtionen respekteras liksom de berörda personernas rätt att invända, uppgifternas säkerhet och riktighet samt att uppgifterna utplånas efter en lämplig tidsperiod.

Utfärdat i Bryssel den 10 februari 2012.

Giovanni BUTTARELLI  
*Biträdande Europeisk datatillsynsman*

---