Yttrande från Europeiska datatillsynsmannen om förslaget till Europaparlamentets och rådets förordning om integritet och öppenhet på energimarknaderna

(2011/C 279/03)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT 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 ([1]), och

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 ([2]), särskilt artikel 41.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING

1. Den 8 december 2010 antog Europeiska kommissionen ett förslag till Europaparlamentets och rådets förordning om integritet och öppenhet på energimarknaderna ([3]) (”förslaget”).

2. Kommissionen samrådde inte med Europeiska datatillsynsmannen, trots att detta krävs enligt artikel 28.2 i förordning (EG) nr 45/2001. Datatillsynsmannen har handlat på eget initiativ och antagit detta yttrande i enlighet med artikel 41.2 i samma förordning. Datatillsynsmannen är medveten om att detta råd kommer i ett sent skede av lagstiftningsförfarandet, men anser likväl att det är lämpligt och av värde att framföra detta yttrande, eftersom förslaget kan få stor betydelse för rätten till integritet och skydd av personuppgifter. En hänvisning till detta yttrande bör införas i ingressen i förslaget.

3. Huvudsyftet med förslaget är att förhindra marknadspåverkan och insiderhandel på grossistmarknaderna för energi (gas och elektricitet). Marknadsintegritet och öppenhet på grossistmarknaderna, där det bedrivs handel med gas och elektricitet mellan energiproducerande företag och näringsidkare, är av avgörande betydelse för konsumenternas slutpris.

4. Syftet med detta förslag är därför att fastställa omfattande bestämmelser på EU-nivå för att förhindra näringsidkare från att använda insiderinformation till sin egen fördel samt från att på ett konstlat sätt påverka priserna att ligga på en nivå som inte motiveras av den faktiska tillgången och kostnaderna för produktion, lagring och transportkapacitet. Enligt de föreslagna bestämmelserna ska framför allt följande förbjudas:

— Utnyttjande av insiderinformation när energi säljs eller köps på grossistmarknader för energi. Exklusiv och priskänslig information ska offentliggöras innan handeln kan äga rum.

— Transaktioner som ger eller kan förväntas ge falska eller vilseledande signaler om tillgång, efterfrågan eller pris på grossistenergiprodukter.

— Spridning av falska nyheter eller rykten som ger vilseledande signaler om dessa produkter.

5. Europeiska byrån för samarbete mellan energitillsynsmyndigheter (nedan kallad *Acer*) ([4]) ansvarar för marknadsövervakningen på europeisk nivå som har till syfte att avslöja eventuella överträdelser av dessa förbud.

6. Enligt förslaget ska Acer ha tillgång till aktuella uppgifter om transaktioner som äger rum på grossistmarknaderna för energi. Detta omfattar uppgifter om pris, såld kvantitet och berörda parter. Dessa bulkdata kommer också att spridas till de nationella tillsynsmyndigheterna, som därefter har ansvaret för att misstänkt missbruk utreds. I ärenden med gränsöverskridande inverkan ska Acer ha befogenhet att samordna undersökningarna. De nationella tillsynsmyndigheterna i medlemsstaterna ska verkställa sanktioner.

7. Förslaget är i linje med en rad andra aktuella lagstiftningsförslag som syftar till att stärka det befintliga finansiella tillsynssystemet samt förbättra samordningen och samarbetet på EU-nivå, däribland direktivet om insiderhandel och otillbörlig marknadspåverkan ([5]) och direktivet om

([1]) EGT L 281, 23.11.1995, s. 31 (nedan kallat direktiv 95/46/EG).
([2]) EGT L 8, 12.1.2001, s. 1 (nedan kallad förordning (EG) nr 45/2001).
([3]) KOM(2010) 726 slutlig.
([4]) Acer är ett EU-organ som inrättades 2010. Det har till uppgift att bistå nationella energitillsynsmyndigheter genom att på EU-nivå utföra de reglerande uppgifter som dessa utför i medlemsstaterna samt vid behov samordna deras åtgärder.
([5]) Europaparlamentets och rådets direktiv 2003/6/EG av den 28 januari 2003 om insiderhandel och otillbörlig marknadspåverkan (marknadsmissbruk), EUT L 96, 12.4.2003, s. 16.

marknader för finansiella instrument ([1]). Europeiska datatillsynsmannen inkom nyligen med synpunkter när det gäller ett annat av dessa aktuella förslag ([2]).

II. EUROPEISKA DATATILLSYNSMANNENS SYNPUNKTER OCH REKOMMENDATIONER

8. Förslaget innehåller flera olika bestämmelser som är relevanta för skyddet av personuppgifter:

— Artiklarna 6–8 om marknadsövervakning och rapportering.

— Artikel 9 om ”uppgiftsskydd och driftssäkerhet”.

— Artiklarna 10 och 11 om utredningar och verkställighet.

— Artikel 14 om ”relationer med tredjeländer”.

II.1 Marknadsövervakning och rapportering (artiklarna 6–8)

Relevanta bestämmelser

9. Förslaget bygger på premissen att för att marknadsmissbruk ska kunna upptäckas i) behövs det en marknadsövervakningsfunktion som har tillgång till fullständiga och aktuella transaktionsuppgifter och att ii) detta ska omfatta övervakning på EU-nivå. Genom förslaget till förordning ges därför Acer befogenhet att samla in, analysera och utbyta uppgifter (tillsammans med relevanta nationella myndigheter och EU-myndigheter) om en stor mängd bulkdata från grossistmarknaderna för energi.

10. I förslaget till förordning fastställs framför allt att marknadsaktörerna ska förse Acer med ”register över deras transaktioner” som rör grossistenergiprodukter. Utöver transaktionsregistren ska marknadsaktörerna också förse Acer med uppgifter om ”anläggningars kapacitet att producera, lagra, förbruka eller överföra el eller naturgas”.

11. I vilken form och vid vilken tidpunkt uppgifterna ska lämnas samt vad de ska innehålla ska fastställas i delegerade akter från kommissionen.

Europeiska datatillsynsmannens synpunkter och rekommendationer

12. Eftersom innehållet i den information som ska samlas in i samband med denna övervakning och rapportering enligt förslaget uteslutande ska fastställas genom delegerade akter, kan det inte uteslutas att detta kommer att omfatta personuppgifter – dvs. varje upplysning som avser en identifierad eller identifierbar fysisk person ([3]). Enligt gällande EU-lagstiftning är detta endast tillåtet när detta är nödvändigt och står i proportion till det specifika syftet ([4]). I förslaget till förordning bör det därför klart anges om och i vilken omfattning som transaktionsregistren och de uppgifter om kapacitet som ska samlas in i övervakningssyfte får omfatta några personuppgifter ([5]).

13. Om behandling av personuppgifter planeras, kan det också vara nödvändigt med särskilda garantier – till exempel när det gäller begränsning av syfte, lagringsperiod och potentiella mottagare av informationen. Eftersom dessa dataskyddsgarantier är av avgörande betydelse ska de i så fall fastställas direkt i förslaget till förordning snarare än i de delegerade akterna.

14. Om det däremot inte beräknas bli aktuellt med någon behandling av personuppgifter (eller om en sådan behandling endast skulle ske i undantagsfall och då endast i de sällsynta fall när en näringsidkare på grossistmarknaden för energi skulle vara en enskild person och inte en juridisk person), bör detta klart anges i förslaget, åtminstone i ett skäl.

II.2 Uppgiftsskydd och driftssäkerhet (artikel 9)

Relevanta bestämmelser

15. Enligt artikel 9.1 ska Acer ”säkerställa sekretess, tillförlitlighet och skydd” för de uppgifter byrån tar emot enligt artikel 7 (dvs. transaktionsregister och uppgifter om kapacitet som samlas in inom ramen för marknadsövervakningen). I artikel 9 fastställs också att ”där så är tillämpligt” ska Acer ”efterleva” förordning (EG) nr 45/2001 när byrån behandlar personuppgifter enligt artikel 7.

16. Enligt artikel 9.1 ska Acer också ”identifiera hot mot driftssäkerheten och minimera dem genom att utveckla lämpliga system, kontroller och förfaranden”.

17. I artikel 9.2 fastställs slutligen att byrån kan besluta om att offentliggöra en del av de uppgifter den besitter, ”under förutsättning att den inte röjer kommersiellt känsliga uppgifter om enskilda marknadsaktörer eller enskilda transaktioner”.

([1]) Europaparlamentets och rådets direktiv 2004/39/EG av den 21 april 2004 om marknader för finansiella instrument och om ändring av rådets direktiv 85/611/EEG och 93/6/EEG och Europaparlamentets och rådets direktiv 2000/12/EG samt upphävande av rådets direktiv 93/22/EEG, EUT L 145, 30.4.2004, s. 1.

([2]) För mer information om det större sammanhanget bakom anknytande lagstiftningsförslag, se Europeiska datatillsynsmannens yttrande om förslaget till Europaparlamentets och rådets förordning om OTC-derivat, centrala motparter och transaktionsregister, som utfärdades den 19 april 2011, särskilt punkterna 4, 5 och 17–20.

([3]) Se artikel 2 a i direktiv 95/46/EG och artikel 2 a i förordning (EG) nr 45/2001.

([4]) Se artiklarna 6.1 c och 7 c i direktiv 95/46/EG och artiklarna 4.1 c och 5 b i förordning (EG) nr 45/2001.

([5]) I artikel 9.1 i förslaget – som innehåller en hänvisning till förordning (EG) nr 45/2001 – antyds att så kan vara fallet, men där ges ingen ytterligare information. Läs mer i avsnitt II.2 i detta yttrande.

Europeiska datatillsynsmannens synpunkter och rekommendationer

18. Datatillsynsmannen välkomnar att artikel 9 till viss del avser dataskydd och att förslaget till förordning innehåller ett specifikt krav om att Acer ska efterleva förordning (EG) nr 45/2001.

a) Tillämpligheten för förordning (EG) nr 45/2001 och direktiv 95/46/EG

19. Därefter understryker datatillsynsmannen att förordning (EG) nr 45/2001 enligt samma förordning är tillämplig för Acer fullt ut så snart byrån behandlar personuppgifter. I förslaget ska det därför erinras om att förordning (EG) nr 45/2001 ska vara tillämplig för Acer inte bara när byrån behandlar uppgifter enligt artikel 7, utan även i alla andra situationer: även när Acer behandlar personuppgifter om misstänkt marknadsmissbruk/överträdelser enligt artikel 11, vilket är viktigt att ange. För att klargöra det hela ytterligare rekommenderar datatillsynsmannen att frasen ”så snart personuppgifter behandlas” används i stället för begreppet ”där så är tillämpligt” när man beskriver de situationer då Acer måste efterleva förordning (EG) nr 45/2001.

20. Det bör också finnas en hänvisning till direktiv 95/46/EG med tanke på att detta direktiv är tillämpligt på de berörda nationella tillsynsmyndigheternas behandling av personuppgifter. För tydlighetens skull rekommenderar datatillsynsmannen att det i förslaget till förordning ska finnas en allmän formulering (åtminstone i ett skäl) om att Acer omfattas av förordning (EG) nr 45/2001, medan direktiv 95/46/EG ska tillämpas på de berörda nationella tillsynsmyndigheterna.

b) Ansvarighet

21. Europeiska datatillsynsmannen välkomnar kravet att Acer ska identifiera hot mot driftssäkerheten och minimera dem genom att utveckla lämpliga system, kontroller och förfaranden. För att ytterligare stärka principen om ansvarighet ([1]) för den händelse att behandlingen av personuppgifter skulle vara av strukturell betydelse, bör förslaget till förordning innehålla ett specifikt krav på att Acer ska fastställa ett tydligt ansvarighetssystem som säkerställer att dataskyddet efterlevs samt styrker detta. Detta tydliga system som har inrättats av Acer bör omfatta flera olika delar. Några exempel:

— Anta samt vid behov uppdatera en dataskyddspolicy på grundval av en konsekvensbedömning (som även ska inbegripa en riskbedömning). Denna dataskyddspolicy bör även omfatta en säkerhetsplan.

— Utföra återkommande granskningar för att kontrollera att dataskyddspolicyn alltjämt är adekvat och efterlevs (inbegriper även en granskning av säkerhetsplanen).

— Offentliggöra resultaten av dessa granskningar (åtminstone till viss del) för att på nytt försäkra aktörerna om att dataskyddet efterlevs.

— Anmäla dataöverträdelser och andra säkerhetsincidenter till kommissionens uppgiftsskyddsombud, berörda registrerade personer samt till andra aktörer och myndigheter när detta är relevant ([2]).

22. Motsvarande krav bör även tillämpas på nationella tillsynsmyndigheter och andra berörda EU-myndigheter.

c) Acers offentliggörande av information

23. När det gäller kravet i artikel 9.2 – att Acer ska offentliggöra en del av den information som byrån besitter – förstår datatillsynsmannen det som att syftet med denna bestämmelse inte är att ge Acer befogenhet att offentliggöra uppgifter för att namnge vem som ligger bakom i skuldbeläggande syfte eller att offentliggöra företags eller enskilda personers förseelser.

24. I förslaget sägs inget om huruvida man har för avsikt att offentliggöra några personuppgifter. För att undanröja alla tvivel bör det i förslaget till förordning antingen specifikt anges att den offentliggjorda informationen inte ska innehålla några personuppgifter eller också bör det klargöras vilka eventuella personuppgifter som får offentliggöras.

25. Om personuppgifter ska offentliggöras, måste behovet av offentliggörande (till exempel av öppenhetsskäl) noggrant övervägas och balanseras mot andra konkurrerande intressen, som behovet att skydda rätten till integritet samt att skydda de berörda personernas personuppgifter.

26. Före varje offentliggörande bör en proportionalitetsbedömning utföras, med hänsyn till de kriterier som EU-domstolen fastställde i målet *Schecke* ([3]). I detta mål underströk domstolen att undantag och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är absolut nödvändigt. Vidare ansåg domstolen att EU-institutionerna bör

([1]) Se avsnitt 7 i Europeiska datatillsynsmannens yttrande om kommissionens meddelande till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén – ”Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen”, som utfärdades den 14 januari 2011 (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf).

([2]) Se avsnitt 6.3 i Europeiska datatillsynsmannens yttrande av den 14 januari 2011 enligt ovan.

([3]) EU-domstolens dom av den 9 november 2010 i de förenade målen C-92/09 och C-93/09 (*Schecke och Eifert*), se särskilt punkterna 81, 65 och 86.

undersöka olika metoder att offentliggöra uppgifter för att fastställa vilken metod som skulle överensstämma med syftet för offentliggörandet och samtidigt orsaka minst ingrepp i de registrerade personernas rätt till integritet samt skyddet av personuppgifter.

II.3 **Utredningsbefogenheter (artikel 10)**

Relevanta bestämmelser

27. Enligt förslaget ska marknadsövervakningen följas av en utredning när det finns misstanke om marknadsmissbruk och detta kan leda till lämpliga påföljder. I artikel 10.1 fastställs framför allt att medlemsstaterna ska se till att de nationella tillsynsmyndigheterna har de utredningsbefogenheter som de behöver för att säkerställa att förordningens bestämmelser om insiderhandel och otillbörlig marknadspåverkan tillämpas ([1]).

Europeiska datatillsynsmannens synpunkter och rekommendationer

28. Europeiska datatillsynsmannen välkomnar klargörandet i artikel 10.1 om att i) utredningsbefogenheterna ska utövas (endast) i syfte att se till att förordningens bestämmelser om insiderhandel och otillbörlig marknadspåverkan (artiklarna 3 och 4) tillämpas samt att ii) dessa befogenheter ska utövas på ett proportionerligt sätt.

29. Men i förslaget bör man gå längre än så för att garantera rättssäkerhet och en adekvat skyddsnivå för personuppgifter. Som beskrivs närmare längre fram finns det två huvudsakliga problem med artikel 10 i dess lydelse enligt förslaget. För det första klargörs inte utredningsbefogenheternas omfattning tillräckligt i artikel 10. Det framgår till exempel inte tillräckligt tydligt om privata teleregister kan begäras in eller om en inspektion på plats får utföras i en privatbostad. För det andra omfattar artikel 10 inte heller de nödvändiga rättssäkerhetsgarantierna mot risken för obefogade intrång i integriteten eller missbruk av personuppgifter. Det ställs till exempel inga krav på en fullmakt från en rättslig myndighet.

30. Såväl utredningsbefogenheternas omfattning som de nödvändiga rättssäkerhetsgarantierna är något som förmodligen ska specificeras i den nationella lagstiftningen. Enligt artikel 10.1 har medlemsstaterna också flera olika alternativ eftersom det här fastställs att utredningsbefogenheterna ”får utövas a) direkt, b) i samarbete med andra myndigheter eller marknadsföretag, eller c) efter ansökan till de behöriga rättsliga myndigheterna”. Detta förefaller innebära att det är tillåtet med skillnader i nationell praxis, till exempel om och under vilka omständigheter som det skulle krävas en fullmakt från en rättslig myndighet.

31. I viss nationell lagstiftning kan det redan förekomma adekvata rättssäkerhets- och dataskyddsgarantier, men för att säkerställa rättssäkerheten för de registrerade, bör vissa klargöranden göras och vissa minimikrav för rättssäkerhets- och dataskyddsgarantier fastställas på EU-nivå i förslaget till förordning, vilket behandlas närmare nedan.

32. Som allmän princip betonar datatillsynsmannen att när det i EU-lagstiftningen ställs krav på att medlemsstaterna ska vidta åtgärder på nationell nivå som inverkar på de grundläggande rättigheterna (till exempel rätten till integritet och rätten till skydd av personuppgifter), ska det i lagstiftningen också ställas krav på att effektiva åtgärder ska vidtas samtidigt med de restriktiva åtgärderna. På så sätt ska det säkerställas att dessa grundläggande rättigheter skyddas. En harmonisering av sådana åtgärder som skulle kunna medföra ingrepp i integriteten, till exempel utredningsbefogenheter, bör med andra ord åtföljas av en harmonisering av adekvata rättssäkerhets- och dataskyddsgarantier, baserat på bästa praxis.

33. En sådan strategi skulle kunna bidra till att förhindra att det blir alltför stora skillnader på nationell nivå och säkerställa en högre och mer enhetlig skyddsnivå för personuppgifter i hela EU.

34. Om det i det här skedet inte är möjligt att harmonisera några minimigarantier, rekommenderar datatillsynsmannen åtminstone att förslaget till förordning bör omfatta ett specifikt krav att medlemsstaterna ska anta nationella genomförandeåtgärder i syfte att säkerställa de nödvändiga rättssäkerhets- och dataskyddsgarantierna. Detta har ännu större betydelse eftersom den form av rättsakt som har valts är en förordning, som är direkt tillämplig och det normalt inte nödvändigtvis skulle krävas några ytterligare genomförandebestämmelser i medlemsstaterna.

II.4 **Inspektioner på plats (artikel 10.2 c)**

Relevanta bestämmelser

35. Enligt förslaget ska de utredningsbefogenheter som ska tilldelas de nationella tillsynsmyndigheterna specifikt omfatta rätten att utföra inspektioner på plats (artikel 10.2 c).

Europeiska datatillsynsmannens synpunkter och rekommendationer

36. Det är inte klart om dessa inspektioner skulle vara begränsade till en marknadsaktörs verksamhetstillgångar (lokaler, mark och transportmedel) eller om de även får utföras i enskilda personers privata egendom (lokaler, mark eller transportmedel). Det är också oklart om inspektionerna får utföras även utan förvarning (”gryningsräder”).

37. Om kommissionen har för avsikt att kräva att medlemsstaterna ska ge tillsynsmyndigheterna befogenhet att utföra utföra inspektioner på plats i enskilda personers privata egendom eller att utföra gryningsräder bör detta för det första klart anges.

([1]) Det bör noteras att Acer inte tilldelas sådana utredningsbefogenheter genom förslaget till förordning. Några sådana befogenheter föreskrivs inte heller för Acer i Europaparlamentets och rådets förordning (EG) nr 713/2009 av den 13 juli 2009 om inrättande av en byrå för samarbete mellan energitillsynsmyndigheter, EUT L 211, 14.8.2009, s. 1.

38. För det andra understryker datatillsynsmannen också att proportionaliteten i inspektioner som utförs på plats i en privat egendom (till exempel en enskild persons privatbostad) är allt annat än självklar och – om detta planeras – bör det också särskilt motiveras.

39. För det tredje skulle det i så fall också krävas ytterligare garantier, särskilt när det gäller under vilka villkor som sådana inspektioner får utföras. I förslaget bör det till exempel utan någon begränsning anges att inspektion på plats endast får utföras om det finns en rimlig och specifik misstanke om att det i denna bostad finns bevismaterial som är relevant för att styrka en allvarlig överträdelse av artiklarna 3 eller 4 i förordningen (dvs. bestämmelserna om förbud mot insiderhandel och otillbörlig marknadspåverkan). En annan viktig sak är att det enligt förslaget också bör krävas en rättslig fullmakt i samtliga medlemsstater ([1]).

40. För det fjärde bör oanmälda inspektioner i privata bostäder kopplas till en ytterligare förutsättning, nämligen att om det gäller ett anmält besök skulle bevismaterialet sannolikt förstöras eller ändras. Genom denna förutsättning blir det möjligt att säkerställa proportionalitet och förhindra överdrivna intrång i privatlivet. Detta bör klart anges i förslaget till förordning.

II.5 **Befogenheter att begära ”befintliga register över tele- och datatrafik” (artikel 10.2 d)**

Relevanta bestämmelser

41. Enligt artikel 10.2 d ska de nationella tillsynsmyndigheternas befogenheter även specifikt omfatta befogenheten att ”begära befintliga register över tele- och datatrafik”.

Europeiska datatillsynsmannens synpunkter och rekommendationer

42. Datatillsynsmannen inser värdet av register över tele- och datatrafik i fall av insiderhandel, särskilt när det gäller att fastställa kopplingar mellan insiderhandlare och näringsidkare. Omfattningen av denna befogenhet har inte klargjorts tillräckligt och det saknas också lämpliga rättssäkerhets- och dataskyddsgarantier. Datatillsynsmannen rekommenderar därför att förslaget klargörs, såsom diskuteras nedan. Det är framför allt följande frågor som bör behandlas:

a) Vilken typ av register över tele- och datatrafik kan begäras?

43. För rättssäkerhetens skull bör det i förslaget först och främst klargöras vilka typer av register som kan begäras in av myndigheterna när detta är nödvändigt.

44. I förslaget bör utredningsbefogenheternas omfattning specifikt begränsas till i) innehållet i register över tele-, e-post- och annan datatrafik som av affärsskäl redan rutinmässigt och lagligt samlas in av näringsidkare i syfte att styrka transaktioner, samt till ii) trafikdata (dvs. vem som har ringt telefonsamtalet eller sänt informationen, till vem och när) som redan är tillgängliga direkt från de berörda marknadsaktörerna (näringsidkarna).

45. I förslaget bör det också anges att dessa register ska ha samlats in i ett lagligt syfte och i enlighet med tillämplig dataskyddslagstiftning, vilket även omfattar adekvat information till de registrerade personerna enligt artiklarna 10 och 11 i direktiv 95/46/EG.

b) Vad avser villkoret ”befintliga”?

46. Datatillsynsmannen välkomnar att denna befogenhet i förslaget är begränsad till ”befintliga” register och att tillsynsmyndigheternas befogenheter därmed inte innebär att en näringsidkare eller tredje man måste åläggas att specifikt avlyssna, övervaka eller registrera tele- eller datatrafik i utredningssyfte.

47. Men för att undanröja alla tvivel bör denna avsikt klargöras i högre grad, åtminstone i ett skäl. Man bör undvika allt tolkningsutrymme för att förslaget till förordning ska utgöra rättslig grund för nationella tillsynsmyndigheter att avlyssna, övervaka eller registrera tele- eller datakommunikation, oavsett om detta sker förtäckt eller öppet, med eller utan fullmakt.

c) Kan innehållet i telefonsamtal och datatrafik också begäras in eller endast trafikdata?

48. I förslaget hänvisas till ”befintliga register över tele- och datatrafik”. Det klargörs inte tillräckligt om både innehållet i befintlig data- och telekommunikation och trafikdata (dvs. vem som ringde samtalet eller sände informationen, till vem och när) kan begäras in.

49. Detta bör förtydligas i bestämmelserna i förslaget till förordning. Såsom diskuteras i punkterna 43–45 bör det tydligt anges vilken typ av register som kan begäras in och det måste först och främst säkerställas att dessa register har samlats in i enlighet med tillämplig dataskyddslagstiftning.

d) Kan register begäras in från internettjänsteleverantörer och telekomföretag?

50. I förslaget bör det entydigt anges vem de nationella tillsynsmyndigheterna får begära in register från. I detta sammanhang förstår datatillsynsmannen det som att avsikten med artikel 10.2 d inte är ge de nationella myndigheterna befogenhet att begära in trafikdata från leverantörer av

([1]) Se till exempel Europadomstolens dom av den 25 februari 1993 i målet *Funke* mot *France* (mål nr 82/1991/334/407), punkterna 55–57.

”allmänt tillgängliga elektroniska kommunikationstjänster” ([1]) (som telekomföretag eller internettjänsteleverantörer).

51. I förslaget hänvisas det inte alls till sådana leverantörer och här används inte heller begreppet ”trafikdata”. En annan viktig sak är att det varken finns någon implicit eller explicit hänvisning till att undantag skulle begäras från de krav som fastställs genom direktivet om integritet och elektronisk kommunikation ([2]), där den allmänna principen om att trafikdata endast får vidarebearbetas som underlag för räkningar och samtrafikfakturor fastställs.

52. För att undanröja alla tvivel rekommenderar datatillsynsmannen att det faktum att förslaget inte utgör någon rättslig grund för att begära in data från leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster bör anges explicit i förslaget till förordning, åtminstone i ett skäl.

e) Kan register begäras in från annan tredje man?

53. I förslaget bör det också klargöras om de nationella tillsynsmyndigheterna endast får begära in register från den marknadsaktör som är under utredning eller om de även har befogenhet att begära in register från tredje man (till exempel från en part i en transaktion med den marknadsaktör som är under utredning eller ett hotell där en enskild person misstänkt för insiderhandel har bott) som då ska lämna sina egna register.

f) Kan några privata register begäras in?

54. I förslaget ska det slutligen också klargöras om myndigheterna även kan begära in enskilda personers privata register. Det kan röra sig om personal eller chefer hos den marknadsaktör som är under utredning (till exempel sms-meddelanden som har sänts från den personliga mobiltelefonen eller sökhistoriken som finns lagrad i hemmadatorn efter internetanvändning i hemmet).

55. Proportionaliteten när det gäller att begära in privata register är omdiskuterad och – om detta planeras – bör det särskilt motiveras.

56. Liksom när det gäller inspektioner som utförs på plats (se punkterna 35–40 ovan) ska det i förslaget ställas krav på en fullmakt från en rättslig myndighet samt ytterligare specifika garantier om myndigheterna begär in några privata register.

II.6 **Rapportering av misstänkt marknadsmissbruk (artikel 11): begränsning av syfte och lagring av uppgifter**

Relevanta bestämmelser

57. När det gäller gränsöverskridande samarbete tilldelas Acer en viktig roll i fråga om att underrätta nationella tillsynsmyndigheter om eventuellt marknadsmissbruk och underlätta informationsutbyte. För att underlätta samarbetet innehåller artikel 11.2 också ett specifikt krav om att de nationella tillsynsmyndigheterna ska underrätta Acer ”så noggrant som möjligt” om de har rimliga skäl att anta någon överträdelse av förslaget till förordning. I syfte att garantera att enhetliga åtgärder vidtas omfattar artikel 11.3 också ett krav på informationsutbyte mellan nationella tillsynsmyndigheter, behöriga finansmyndigheter, Acer samt Europeiska värdepappers- och marknadsmyndigheten (nedan kallad *Esma*) ([3]).

Europeiska datatillsynsmannens synpunkter och rekommendationer

58. I enlighet med principen om att begränsa syftet ([4]) bör det i förslaget explicit anges att alla personuppgifter som har överförts med stöd av artikel 11 i förslaget till förordning (rapporter om misstänkt marknadsmissbruk) endast bör användas för att utreda det misstänkta marknadsmissbruk som har rapporterats. Informationen får hur som helst inte användas till några syften som är oförenliga med detta ändamål.

59. Uppgifterna bör heller inte lagras under lång tid. Detta är särskilt viktigt i fall där det visar sig att den ursprungliga misstanken var grundlös, då det måste krävas särskilda skäl för att lagra uppgifterna under längre tid ([5]).

60. Med avseende på detta bör det i förslaget först fastställas en längsta lagringstid som Acer och andra mottagare av informationen får behålla uppgifterna, med hänsyn till de ändamål för vilka de ska lagras. Om ett misstänkt marknadsmissbruk inte har lett till en särskild utredning, och denna fortfarande pågår, bör alla personuppgifter som avser det rapporterade misstänkta marknadsmissbruket raderas från alla mottagares register efter en viss tid. Om det inte är tydligt motiverat med en längre lagringsperiod, anser

([1]) Se artikel 2 c i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv), EGT L 108, 24.4.2002, s. 33.

([2]) Se artikel 6.1 i 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.

([3]) Esma är en oberoende EU-myndighet som bidrar till att skydda stabiliteten i EU:s finansiella system genom att säkerställa integritet, öppenhet, effektivitet och välordnad funktion på värdepappersmarknaden, samt att stärka skyddet för investerare.

([4]) Se artikel 6.1 b i direktiv 95/46/EG och artikel 4.1 b i förordning (EG) nr 45/2001.

([5]) Europeiska datatillsynsmannen vill i detta sammanhang till exempel hänvisa till domen från Europadomstolen i målet *S. och Marper* mot *Förenade kungariket* (2008) (4 december 2008) (ansökningar nr 30562/04 och 30566/04), där det slogs fast att det var ett brott mot rätten till integritet enligt artikel 8 i Europeiska konventionen om mänskliga rättigheter att under lång tid lagra uppgifter om personer som inte har dömts för något brott.

datatillsynsmannen att de bör raderas senast två år efter den tidpunkt då misstanken rapporterades ([1]).

61. Skulle en misstanke visa sig vara ogrundad och/eller en utredning avslutas utan vidare åtgärd, ska den rapporterande tillsynsmyndigheten, Acer samt tredje man med tillgång till information om misstänkt marknadsmissbruk enligt förslaget åläggas att snabbt underrätta dessa parter så att de kan uppdatera sina egna register om detta (och/eller radera informationen om den rapporterade misstanken från sina register med omedelbar verkan eller efter en proportionerlig lagringsperiod, beroende på vad som är lämpligt) ([2]).

62. Dessa bestämmelser bör bidra till att oskyldiga inte ”svartlistas” eller förblir misstänkta under onödigt lång tid (se artikel 6 e i direktiv 95/46/EG och motsvarande artikel 4 e i förordning (EG) nr 45/2001) i fall där misstanken inte har kunnat styrkas (eller ens utretts vidare).

II.7 **Dataöverföringar till tredjeländer (artikel 14)**

Relevanta bestämmelser

63. Artiklarna 7, 8 och 11 i förslaget till förordning avser utbyte av data och information mellan Acer, Esma och medlemsstaternas myndigheter. I artikel 14 (”Relationer med tredjeländer”) föreskrivs att Acer ”får inleda administrativa förfaranden med internationella organisationer och myndigheter i tredjeländer”. Detta kan leda till överföring av personuppgifter från Acer och möjligtvis även från Esma och/eller från medlemsstaternas myndigheter till internationella organisationer och myndigheter i tredjeländer.

Europeiska datatillsynsmannens synpunkter och rekommendationer

64. Europeiska datatillsynsmannen rekommenderar att artikel 14 i förslaget klargör att överföringar av personuppgifter endast får göras i enlighet med artikel 9 i förordning (EG) nr 45/2001 och artiklarna 25 och 26 i direktiv 95/46/EG. Framför allt ska internationella överföringar endast genomföras om tredjelandet i fråga garanterar en adekvat skyddsnivå eller om de riktar sig till enheter eller enskilda personer i ett tredjeland som inte kan bekosta adekvat skydd där den registeransvarige ställer tillräckliga garantier för att integritet och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter.

65. Datatillsynsmannen understryker att undantag (till exempel sådana som anges i artikel 9.6 i förordning (EG) nr 45/2001 och artikel 26.1 i direktivet), principiellt sett inte ska användas för att motivera överföringar av mass-, system- och/eller strukturdata till tredjeland.

II.8 **Förhandskontroll av Acers samordnande verksamhet i fråga om utredningar**

66. Vissa av de data som utbyts mellan Acer, Esma och olika myndigheter i medlemsstaterna om misstänkta överträdelser kommer sannolikt att innehålla personuppgifter som identiteten på misstänkta förövare eller andra involverade personer (till exempel vittnen, personer som slagit larm om missförhållanden, anställda eller andra enskilda personer som agerar för de företag som är involverade i handeln).

67. I artikel 27.1 i förordning (EG) nr 45/2001 föreskrivs att ”sådana behandlingar som kan innebära särskilda risker för de registrerades fri- och rättigheter på grund av sin beskaffenhet, sin räckvidd eller sina ändamål skall förhandskontrolleras av den europeiska datatillsynsmannen”. I artikel 27.2 bekräftas specifikt att behandling av uppgifter som rör ”misstankar om brott” och ”brott” utgör sådana risker och kräver förhandskontroll. Med tanke på att Acer är tänkt att få en samordnande roll i utredningsarbetet förefaller det sannolikt att byrån kommer att behandla uppgifter som rör ”misstankar om brott” och att dess verksamhet därför behöver förhandskontrolleras ([3]).

68. Inom ramen för en sådan förhandskontroll kan datatillsynsmannen ge Acer ytterligare vägledning och specifika rekommendationer när det gäller efterlevnaden av reglerna för uppgiftsskydd. En förhandskontroll av Acers verksamhet kan också ge ett mervärde med tanke på att förordning (EG) nr 713/2009, varigenom Acer inrättades, inte innehåller någon hänvisning till skyddet av personuppgifter och inte har varit föremål för något lagstiftningsyttrande från datatillsynsmannen.

III. **SLUTSATSER**

69. I förslaget bör det klargöras om personuppgifter får behandlas i samband med marknadsövervakning och rapportering samt vilka garantier som ska tillämpas. Om det däremot inte beräknas bli aktuellt med någon behandling av personuppgifter (eller om en sådan behandling endast skulle ske i undantagsfall och då endast i de sällsynta fall när en näringsidkare på grossistmarknaden för energi skulle vara en enskild person snarare än en juridisk person), bör detta klart anges i förslaget, åtminstone i ett skäl.

([1]) Om en misstanke visar sig vara välgrundad och leder till en framgångsrik utredning, bör det i förslaget anges en specifik lagringsperiod – som inte är alltför lång – efter det att utredningen har avslutats.

([2]) Denna information bör även tillhandahållas till den registrerade.

([3]) Det bör noteras att även den databehandling som utförs av nationella myndigheter kan behöva förhandskontrolleras av nationella eller regionala dataskyddsmyndigheter enligt den nationella dataskyddslagstiftning som har antagits enligt artikel 20 i direktiv 95/46/EG.

70. Bestämmelserna om dataskydd, datasäkerhet och ansvarighet bör klargöras och stärkas ytterligare, framför allt om behandlingen av personuppgifter skulle få mer strukturell betydelse. Kommissionen bör se till att det finns adekvata kontroller för att säkerställa efterlevnaden av dataskyddet och kunna styrka detta (”ansvarighet”).

71. I förslaget bör det klargöras om inspektionerna på plats skulle vara begränsade till en marknadsaktörs verksamhetstillgångar (lokaler och transportmedel) eller om de även får utföras i enskilda personers privata egendom (lokaler eller transportmedel). I det sistnämnda fallet bör det tydligt motiveras att denna befogenhet är nödvändig och proportionerlig och det ska krävas en rättslig fullmakt och ytterligare garantier. Detta bör klart anges i förslaget till förordning.

72. Befogenheternas omfattning när det gäller att begära in ”befintliga register över tele- och datatrafik” bör klargöras. I förslaget bör det entydigt anges vilka register som kan begäras in och från vem. Att inga data får begäras in från leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster bör anges explicit i förslaget till förordning, åtminstone i ett skäl. I förslaget ska det också klargöras om myndigheterna även kan begära in enskilda personers privata register. Det kan röra sig om personal eller chefer hos den marknadsaktör som är under utredning (till exempel sms-meddelanden som har sänts från den personliga mobiltelefonen eller sökhistoriken som finns lagrad i hemmadatorn efter internetanvändning i hemmet). I så fall bör det tydligt motiveras att denna befogenhet är nödvändig och proportionerlig och enligt förslaget ska det också krävas en fullmakt från en rättslig myndighet.

73. När det gäller rapportering av misstänkt marknadsmissbruk bör det i förslaget explicit anges att personuppgifterna i dessa rapporter endast bör användas för utredning av det misstänkta marknadsmissbruk som har rapporterats. Om ett misstänkt marknadsmissbruk inte har lett till en särskild utredning, och denna fortfarande pågår (eller om en misstanke visar sig vara välgrundad och leder till en framgångsrik utredning), bör alla personuppgifter som avser det rapporterade misstänkta marknadsmissbruket raderas från alla mottagares register efter en viss tid (senast två år efter den tidpunkt då misstanken rapporterades, såvida det inte kan motiveras på annat sätt). Parterna i ett informationsutbyte bör också sända varandra en uppdatering, om en misstanke skulle visa sig vara ogrundad och/eller en utredning avslutas utan vidare åtgärd.

74. När det gäller överföringar av personuppgifter till tredjeland bör det i förslaget klargöras att sådana överföringar i princip endast får genomföras om de riktar sig till enheter eller enskilda personer i ett tredjeland som inte kan bekosta adekvat skydd där den registeransvarige ställer tillräckliga garantier för att integritet och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter.

75. Acer bör lämna sina databehandlingsåtgärder till Europeiska datatillsynsmannen för förhandskontroll när det gäller samordning av utredningar enligt artikel 11 i förslaget till förordning.

Utfärdat i Bryssel den 21 juni 2011.

Giovanni BUTTARELLI

Biträdande Europeisk datatillsynsman