Europeiska unionens
officiella tidning

C 328

Svensk utgåva

sextiosjätte årgången

18 september 2023

Meddelanden och upplysningar

Innehållsförteckning

SV

([1]) Text av betydelse för EES.

([1]) Text av betydelse för EES.

II

(Meddelanden)

MEDDELANDEN FRÅN EUROPEISKA UNIONENS INSTITUTIONER, BYRÅER OCH ORGAN

EUROPEISKA KOMMISSIONEN

Beslut om att inte göra invändningar mot en anmäld koncentration

(Ärende M.11106 – STELLANTIS / MICHELIN / FORVIA / SYMBIO)

(Text av betydelse för EES)

(2023/C 328/01)

Kommissionen beslutade den 17 juli 2023 att inte göra invändningar mot den anmälda koncentrationen ovan och att förklara den förenlig med den inre marknaden. Beslutet grundar sig på artikel 6.1 b i rådets förordning (EG) nr 139/2004 ([1]). Beslutet i sin helhet finns bara på engelska och kommer att offentliggöras efter det att eventuella affärshemligheter har tagits bort. Det kommer att finnas

— under rubriken koncentrationer på kommissionens webbplats för konkurrens (https://competition-cases.ec.europa.eu/search). Denna webbplats gör det möjligt att hitta enskilda beslut i koncentrationsärenden, uppgifter om företag, ärendenummer, datum och sektorer,

— i elektronisk form på webbplatsen EUR-Lex (http://eur-lex.europa.eu/homepage.html?locale=sv) under Celexnummer 32023M11106. EUR-Lex ger tillgång till unionslagstiftningen via internet.

([1]) EUT L 24, 29.1.2004, s. 1.

MEDDELANDE FRÅN KOMMISSIONEN

Kommissionens riktlinjer för tillämpningen av artikel 4.1 och 4.2 i direktiv (EU) 2022/2555 (NIS 2-direktivet)

(2023/C 328/02)

I. INLEDNING

1. I enlighet med artikel 4.3 i Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet) ([1]) ska kommissionen senast den 17 juli 2023 tillhandahålla riktlinjer som klargör tillämpningen av artikel 4.1 och 4.2 i det direktivet.

2. Dessa riktlinjer klargör tillämpningen av dessa bestämmelser, som rör förhållandet mellan direktiv (EU) 2022/2555 och nuvarande och framtida sektorsspecifika unionsrättsakter som omfattar riskhanteringsåtgärder för cybersäkerhet eller incidentrapporteringskrav. I tillägget till dessa riktlinjer förtecknas sektorsspecifika unionsrättsakter som enligt kommissions mening omfattas av artikel 4 i direktiv (EU) 2022/2555. Det faktum att en rättsakt inte förtecknas i detta tillägg innebär inte nödvändigtvis att den inte omfattas av den bestämmelsen.

3. Vid tillämpningen av artikel 4.3 tredje meningen i direktiv (EU) 2022/2555 tog kommissionen hänsyn till synpunkter från samarbetsgruppen för nät- och informationssäkerhet och Europeiska unionens cybersäkerhetsbyrå (Enisa) innan dessa riktlinjer antogs.

4. Riktlinjerna påverkar inte Europeiska unionens domstols tolkning av unionsrätten.

II. SEKTORSSPECIFIKA UNIONSRÄTTSAKTERS LIKVÄRDIGHET MED CYBERSÄKERHETSKRAV

5. I artikel 4.1 i direktiv (EU) 2022/2555 föreskrivs att om det i sektorsspecifika unionsrättsakter föreskrivs att väsentliga eller viktiga entiteter ska anta riskhanteringsåtgärder för cybersäkerhet eller underrätta om betydande incidenter, och om dessa krav har minst samma verkan som de skyldigheter som fastställs i det direktivet, ska de relevanta bestämmelserna i direktiv (EU) 2022/2555, inbegripet bestämmelserna om tillsyn och efterlevnadskontroll i kapitel VII i direktivet, inte tillämpas på sådana entiteter. I artikeln fastställs vidare att om de sektorsspecifika unionsrättsakterna inte omfattar alla entiteter inom en viss sektor som omfattas av tillämpningsområdet för direktiv (EU) 2022/2555, ska de relevanta bestämmelserna i det direktivet fortsätta att tillämpas på de entiteter som inte omfattas av dessa sektorsspecifika unionsrättsakter.

II.1. Riskhanteringskrav för cybersäkerhet

6. I artikel 4.2 a i direktiv (EU) 2022/2555 föreskrivs att de riskhanteringsåtgärder för cybersäkerhet som väsentliga eller viktiga entiteter är ålagda att vidta enligt sektorsspecifika unionsrättsakter ska anses vara likvärdiga med de skyldigheter som fastställs i direktiv (EU) 2022/2555, om dessa krav har minst samma verkan som de skyldigheter som fastställs i artikel 21.1 och 21.2 i det direktivet. När det bedöms om kraven i en sektorsspecifik unionsrättsakt avseende riskhanteringsåtgärder för cybersäkerhet har minst samma verkan som de krav som fastställs i artikel 21.1 och 21.2 i direktiv (EU) 2022/2555, bör kraven i den sektorsspecifika unionsrättsakten minst motsvara kraven i de bestämmelserna eller vara mer långtgående än dessa, vilket innebär att de sektorsspecifika bestämmelserna får vara mer detaljerade i sak än motsvarande bestämmelser i direktiv (EU) 2022/2555.

([1]) EUT L 333, 27.12.2022, s. 80.

7. Enligt artikel 21.1 första stycket i direktiv (EU) 2022/2555 ska medlemsstaterna säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster. Dessa åtgärder bör vara riskbaserade och bör kunna förhindra eller minimera incidenters konsekvenser. I artikel 21.1 andra stycket i direktiv (EU) 2022/2555 specificeras hur sådana åtgärders proportionalitet ska bedömas ([2]). Den skyldighet som fastställs i artikel 21.1 i direktiv (EU) 2022/2555 och som innebär att väsentliga och viktiga entiteter ska vidta lämpliga och proportionella riskhanteringsåtgärder för cybersäkerhet avser den berörda entitetens hela verksamhet och samtliga tjänster, inte bara specifika it-tillgångar eller kritiska tjänster som tillhandahålls av entiteten.

8. Vid bedömningen av en sektorsspecifik unionsrättsakts likvärdighet med de relevanta bestämmelserna om cyberriskhantering i direktiv (EU) 2022/2555 bör man särskilt fästa vikt vid om säkerhetskraven enligt den rättsakten omfattar åtgärder som syftar till att säkerställa säkerheten i nätverks- och informationssystem. Definitionen av ”säkerhet i nätverks- och informationssystem”, som fastställs i artikel 6.2 i direktiv (EU) 2022/2555, avser nätverks- och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå händelser som skulle kunna undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem. Användningen av begreppen ”tillgänglighet”, ”autenticitet”, ”riktighet” och ”konfidentialitet” i definitionen avser alla fyra skyddsmål som rör säkerheten i nät- och informationssystem. Begreppet ”nätverks- och informationssystem”, enligt definitionen i artikel 6.1 i direktiv (EU) 2022/2555, omfattar elektroniska kommunikationsnät ([3]), en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, och digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana elektroniska kommunikationsnät eller enheter för att de ska kunna drivas, användas, skyddas och underhållas. Därför bör de säkerhetsåtgärder som krävs enligt en sektorsspecifik unionsrättsakt också omfatta hårdvara, fast programvara och programvara som används för en enhets drift.

9. Ett annat viktigt övervägande vid bedömning av en sektorsspecifik unionsrättsakts likvärdighet med kraven i artikel 21.1 och 21.2 i direktiv (EU) 2022/2555 är att de riskhanteringsåtgärder för cybersäkerhet som krävs enligt rättsakten bör vara baserade på en ”allriskansats”. Eftersom hot mot säkerheten i nätverks- och informationssystem kan ha olika ursprung kan alla typer av händelser ha en negativ inverkan på entitetens nätverks- och informationssystem och potentiellt leda till en incident. Därför bör de riskhanteringsåtgärder för cybersäkerhet som entiteten vidtar skydda inte bara entitetens nätverks- och informationssystem utan också dessa systems fysiska miljö mot sådana händelser som sabotage, stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysisk åtkomst som kan undergräva tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. Följaktligen bör de riskhanteringsåtgärder för cybersäkerhet som krävs enligt en sektorsspecifik unionsrättsakt specifikt skydda nätverks- och informationssystemens fysiska säkerhet och säkerheten i deras miljö från systemfel, mänskliga misstag, skadliga handlingar eller naturfenomen ([4]).

10. Enligt artikel 21.2 i direktiv (EU) 2022/2555 ska riskhanteringsåtgärderna för cybersäkerhet också inbegripa de specifika cybersäkerhetskrav som anges i artikel 21.2 a-j. Dessa krav omfattar sådana åtgärder som strategier för riskanalys och informationssystemens säkerhet, incidenthantering, driftskontinuitet, krishantering, säkerhet i leveranskedjan samt strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering. Enligt artikel 21.5 andra stycket i direktiv (EU) 2022/2555 har kommissionen befogenhet att anta genomförandeakter för att fastställa tekniska och metodologiska krav samt, vid behov, sektorskrav för de säkerhetsåtgärder som avses i artikel 21.2 i det direktivet. När det gäller leverantörer av DNS-tjänster, registreringsenheter för

([2]) Se även skäl 78, 81 och 82 i direktiv (EU) 2022/2555.

([3]) Artikel 2.1 i Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (EUT L 321, 17.12.2018, s. 36).

([4]) Se skäl 79 i direktiv (EU) 2022/2555.

toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer, plattformar för sociala nätverkstjänster samt kvalificerade tillhandahållare av betrodda tjänster ska kommissionen senast den 17 oktober 2024 anta genomförandeakter med tekniska och metodologiska krav för de säkerhetsåtgärder som avses i artikel 21.2 i direktiv (EU) 2022/2555. Genomförandeakter specificerar mer ingående de viktigaste villkoren och kriterierna för genomförandet enligt grundakten, utan att påverka den akten i sak ([5]).

II.2. **Rapporteringskrav**

11. Enligt artikel 4.2 b i direktiv (EU) 2022/2555 ska rapporteringskraven för underrättelse av betydande incidenter anses ha samma verkan som de krav som fastställs i det direktivet om en sektorsspecifik unionsrättsakt föreskriver omedelbar, och när det är lämpligt automatisk och direkt, tillgång till incidentunderrättelser från CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna och om kraven på underrättelse av betydande incidenter har minst samma verkan som de krav som fastställs i artikel 23.1–23.6 i direktiv (EU) 2022/2555.

12. Eftersom de krav i en sektorsspecifik unionsrättsakt som rör underrättelse av betydande incidenter måste ha minst samma verkan som de krav som fastställs i artikel 23.1–23.6 i direktiv (EU) 2022/2555 för att den akten ska tillämpas i stället för rapporteringsskyldigheterna enligt det direktivet, är de krav som fastställs i artikel 23.1–23.6 särskilt viktiga för bedömningen av likvärdighet. I artikel 23.1–23.6 i direktiv (EU) 2022/2555 fastställs mer detaljerat vilka typer av incidenter som måste rapporteras till vem, inom vilka tidsramar och vad informationen ska omfatta. Detta förklaras mer ingående nedan.

II.2.1. *Underrättelse av betydande incidenter till CSIRT-enheter, behöriga myndigheter och mottagare*

13. Enligt den första meningen i artikel 23.1 första stycket i direktiv (EU) 2022/2555 ska väsentliga och viktiga entiteter utan onödigt dröjsmål underrätta sin CSIRT-enhet eller, i tillämpliga fall, sin behöriga myndighet om alla betydande incidenter. Enligt den andra meningen i artikel 23.1 första stycket i direktiv (EU) 2022/2555 ska väsentliga och viktiga entiteter, när så är lämpligt, utan onödigt dröjsmål underrätta mottagarna av deras tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av de tjänsterna.

14. I artikel 6.6 i direktiv (EU) 2022/2555 ges visserligen en väldigt bred definition av ”incident”, som en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men enligt artikel 23.1 i det direktivet är det endast betydande incidenter som omfattas av en rapporteringsskyldighet. En incident är betydande om den har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten (artikel 23.3 a) eller om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada (artikel 23.3 b).

([5]) Se kapitel D, Ytterligare regler som kompletterar den grundläggande rättsakten, i *Icke bindande kriterier för tillämpningen av artiklarna 290 och 291 i fördraget om Europeiska unionens funktionssätt* — 18 juni 2019 (EUT C 223, 3.7.2019, s. 1).

15. I skäl 101 i direktiv (EU) 2022/2555 klargörs att rapporteringen av incidenter bör baseras på en första bedömning som utförts av den berörda entiteten. En sådan inledande bedömning bör bland annat ta hänsyn till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av entitetens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt entitetens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många tjänstemottagare som drabbas kan spela en viktig roll när man fastställer om tjänstens driftsstörning är allvarlig.

16. I enlighet med artikel 23.11 andra stycket i direktiv (EU) 2022/2555 får kommissionen anta genomförandeakter som närmare anger i vilka fall en incident ska anses vara betydande. När det gäller leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster ska kommissionen senast den 17 oktober 2024 anta sådana genomförandeakter. Genomförandeakter specificerar mer ingående de viktigaste villkoren och kriterierna för genomförandet enligt grundakten, utan att påverka den akten i sak ([6]).

II.2.2. *Flerstegsstrategi och tidsram för rapportering av betydande incidenter*

17. I direktiv (EU) 2022/2555 fastställs en flerstegsstrategi för rapportering av betydande incidenter. Den omfattar en tidig varning, en incidentunderrättelse och en slutrapport. Dessa tre delar kan eventuellt kompletteras med delrapporter och en lägesrapport.

18. Flerstegsstrategin syftar till att hitta rätt balans mellan, å ena sidan, en snabb rapportering som bidrar till att begränsa den potentiella spridningen av betydande incidenter och gör det möjligt för väsentliga och viktiga entiteter att söka bistånd och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och med tiden förbättrar cyberresiliensen hos enskilda entiteter och hela sektorer ([7]).

19. Enligt flerstegsstrategin ska väsentliga och viktiga entiteter som får kännedom om en betydande incident först lämna en in tidig varning till den behöriga CSIRT-enheten eller myndigheten, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar. Sedan ska dessa entiteter lämna in en incidentanmälan, utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten. Därefter kan en behörig CSIRT-enhet eller myndighet begära en delrapport. Slutligen ska en slutrapport lämnas till den behöriga CSIRT-enheten eller myndigheten senast en månad efter att incidentanmälan lämnats in, om inte incidenten fortfarande pågår vid den tidpunkten. I sådana fall ska en lägesrapport tillhandahållas och slutrapporten inlämnas inom en månad efter det att incidenten hanterats.

20. En annan tidsram ska tillämpas på incidentanmälan enligt artikel 23.4 andra stycket i direktiv (EU) 2022/2555 när det gäller tillhandahållare av betrodda tjänster, Dessa tillhandahållare ska anmäla betydande incidenter som påverkar tillhandahållandet av de betrodda tjänsterna, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten.

([6]) Se kapitel D, Ytterligare regler som kompletterar den grundläggande rättsakten, i *Icke bindande kriterier för tillämpningen av artiklarna 290 och 291 i fördraget om Europeiska unionens funktionssätt* — 18 juni 2019 (EUT C 223, 3.7.2019, s. 1).

([7]) Se skäl 101 i direktiv (EU) 2022/2555.

II.2.3. *Innehåll i skyldigheten att rapportera betydande incidenter till CSIRT-enheter eller behöriga myndigheter*

21. I princip innebär artikel 23.1 första stycket tredje meningen i artikel (EU) 2022/2555 att medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter ska rapportera bland annat all information som gör det möjligt för CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten att fastställa incidentens eventuella gränsöverskridande verkningar. Detta krav som rör rapporteringsskyldighetens innehåll specificeras närmare i artikel 23.4 i direktiv (EU) 2022/2555, där flerstegsstrategin fastställs.

22. Enligt artikel 23.4 a ska den tidiga varningen i tillämpliga fall ange om den betydande incidenten misstänks vara orsakad av olagliga eller avsiktligt skadliga handlingar och eller om den skulle kunna få (alltså om det är troligt att den kommer att få) gränsöverskridande verkningar. Enligt skäl 102 i direktiv (EU) 2022/2555 bör den tidiga varningen endast innehålla den information som är nödvändig för att göra den behöriga CSIRT-enheten eller myndigheten, medveten om den betydande incidenten och ge den berörda entiteten möjlighet att vid behov söka bistånd.

23. Incidentanmälan ska, i förekommande fall, omfatta uppdateringar av den information som lämnats via den tidiga varningen. Den ska även omfatta en inledande bedömning av den betydande incidenten, inbegripet dess allvarlighetsgrad och konsekvenser samt angreppsindikatorer, om tillgängliga.

24. I de fall då en delrapport begärs ska den innehålla relevanta statusuppdateringar. Slutrapporten ska innehålla en detaljerad beskrivning av incidenten, inbegripet dess allvarlighetsgrad och konsekvenser, samt av den typ av hot eller grundorsak som sannolikt har utlöst incidenten, tillämpade och pågående begränsande åtgärder och, i förekommande fall, incidentens gränsöverskridande verkningar.

II.2.4. *Omedelbar tillgång till incidentanmälningar*

25. Enligt artikel 4.2 b i direktiv (EU) 2022/2555 måste en sektorsspecifik unionsrättsakt, som ska tillämpas på rapporteringsskyldigheten i stället för det direktivet, ge CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt direktiv (EU) 2022/2555 omedelbar tillgång till incidentunderrättelser som lämnats i enlighet med den sektorsspecifika unionsrättsakten. I enlighet med skäl 24 i direktiv (EU) 2022/2555 kan en sådan omedelbar tillgång säkerställas om incidentanmälningar vidarebefordras utan onödigt dröjsmål till CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten.

26. Omedelbar tillgång kan tillhandahållas genom metoder för automatisk och direkt tillgång, som medlemsstaterna bör inrätta när så är lämpligt. Automatiska och direkta rapporteringsmekanismer säkerställer systematisk och omedelbar informationsdelning med CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna angående hanteringen av sådana incidentanmälningar. Medlemsstaterna får också använda en gemensam kontaktpunkt, som behöver vara förenlig med den sektorsspecifika unionsrättsakten, för att förenkla rapporteringen och genomföra den automatiska och direkta rapporteringsmekanismen.

27. När det bedöms om kraven i en sektorsspecifik unionsrättsakt angående anmälan av betydande incidenter har minst samma verkan som de krav som fastställs i artikel 23.1–23.6 i direktiv (EU) 2022/2555 ska kraven i den sektorsspecifika unionsrättsakten minst motsvara kraven i artikel 23.1–23.6 eller omfatta mer detaljerade krav än de bestämmelserna. Kraven bör avse den typ av incidenter som måste rapporteras i enlighet med direktiv (EU) 2022/2555, med beaktande av i synnerhet mottagarna, innehållet och de tillämpliga tidsramarna.

III. KONSEKVENS OCH LIKVÄRDIGHET

III.1. Tillsyn och efterlevnadskontroll

28. I de fall då sektorsspecifika unionsrättsakter har minst samma verkan som de skyldigheter som fastställs i direktiv (EU) 2022/2555, är det inte bara de berörda bestämmelserna i det direktivet som rör skyldigheten att anta riskhanteringsåtgärder för cybersäkerhet eller anmäla betydande incidenter som inte ska tillämpas, utan även bestämmelserna om tillsyn och efterlevnadskontroll i kapitel VII i direktiv (EU) 2022/2555.

29. I skäl 25 i direktiv (EU) 2022/2555 förklaras att sektorsspecifika unionsrättsakter som minst har samma verkan kan föreskriva att behöriga myndigheter inom ramen för de rättsakterna utövar sina tillsyns- och efterlevnadskontrollbefogenheter avseende riskhanteringsåtgärder för cybersäkerhet eller anmälningsskyldigheter med bistånd av de behöriga myndigheterna inom ramen för direktiv (EU) 2022/2555. De berörda behöriga myndigheterna skulle kunna upprätta samarbetsarrangemang i detta syfte, bland annat när det gäller samordning av tillsynsverksamheten, förfarandena för utredningar och inspektioner på plats i enlighet med nationell rätt och en mekanism för utbyte av relevant information om tillsyn och efterlevnadskontroll mellan de behöriga myndigheterna. En sådan mekanism för utbyte av relevant information skulle kunna innefatta tillgång till cyberrelaterad information som begärs av de behöriga myndigheterna inom ramen för direktiv (EU) 2022/2555.

III.2. Nationell strategi för cybersäkerhet

30. Varje medlemsstat ska anta en nationell strategi för cybersäkerhet i enlighet med artikel 7.1 i direktiv (EU) 2022/2555. En nationell strategi för cybersäkerhet är en enhetlig ram i en medlemsstat med strategiska mål och prioriteringar på cybersäkerhetsområdet och en styrningsram för att uppnå dessa mål och prioriteringar i den medlemsstaten (se artikel 6.4 i direktiv (EU) 2022/2555). Cybersäkerhetsstrategin ska bland annat omfatta mål och prioriteringar för i synnerhet de sektorer som avses i bilagorna I och II i direktiv (EU) 2022/2555. Cybersäkerhetsstrategin ska också omfatta en styrningsram för att uppnå de mål och prioriteringar som avses i artikel 7.2 i direktiv (EU) 2022/2555.

31. I artikel 7.1 c i direktiv (EU) 2022/2555 föreskrivs vidare att den nationella strategin för cybersäkerhet ska omfatta en styrningsram som klargör roller och ansvarsområden för relevanta intressenter på nationell nivå och som stöder samarbetet och samordningen på nationell nivå mellan de behöriga myndigheterna, de gemensamma kontaktpunkterna och CSIRT-enheterna enligt direktiv (EU) 2022/2555, samt samordningen och samarbetet mellan dessa organ och behöriga myndigheter enligt sektorsspecifika unionsrättsakter,

32. Kraven avseende antagandet av en strategi för cybersäkerhet i enlighet med artikel 7 i direktiv (EU) 2022/2555 omfattar följaktligen varken de cybersäkerhetskrav som gäller för väsentliga och viktiga entiteter enligt artiklarna 21 och 23 i det direktivet eller de bestämmelser som rör tillsynen och efterlevnadskontrollen av dessa enligt artikel VII såsom föreskrivs i artikel 4.1 och 4.2 i det direktivet. De berörda bestämmelserna i artikel 7 bör fortsätta att tillämpas på sektorer, delsektorer och typer av entiteter för vilka det finns sektorsspecifika unionsrättsakter i den mening som avses i artikel 4 i direktiv (EU) 2022/2555.

III.3. Utseende av CSIRT-enheter

33. Enligt artikel 10.1 i direktiv (EU) 2022/2555 ska medlemsstaterna utse eller inrätta en eller flera CSIRT-enheter som ska omfatta minst de sektorer, delsektorer och typer av entiteter som avses i bilagorna I och II i det direktivet och därmed innefatta sektorer, delsektorer och typer av entiteter för vilka det finns sektorsspecifika unionsrättsakter. CSIRT-enheterna kommer normalt sett också att utföra sina uppgifter enligt artikel 11.3 i direktiv (EU) 2022/2555 i det avseendet, om inte särskilda uppgifter specificeras i de sektorsspecifika unionsrättsakterna.

III.4. **Nationella ramar för hantering av cybersäkerhetskriser och EU-CyCLONe**

34. Enligt artikel 9.1 i direktiv (EU) 2022/2555 ska medlemsstaterna utse eller inrätta en eller flera cyberkrishanteringsmyndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Enligt artikel 6.7 i det direktivet är en storskalig cybersäkerhetsincident en incident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater. Enligt artikel 9.4 i direktiv (EU) 2022/2555 ska varje medlemsstat också anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser, där mål och villkor för hanteringen av storskaliga cybersäkerhetsincidenter och kriser fastställs. I denna plan bör man bland annat fastställa cyberkrishanteringsförfaranden, inbegripet integreringen av dessa i den allmänna nationella ramen för krishantering och kanaler för informationsutbyte, samt berörda offentliga och privata intressenter och berörd infrastruktur. Sådana cyberkrishanteringsförfaranden och berörda offentliga och privata intressenter och berörd infrastruktur kan innefatta sektorsspecifika förfaranden och intressenter.

35. Genom artikel 16 i direktiv (EU) 2022/2555 inrättas det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) som ska stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på operativ nivå och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer.

36. Artikel 9 om ramar för hantering av cybersäkerhetskriser och artikel 16 om EU-CyCLONe rör inte de cybersäkerhetskrav som gäller för entiteter enligt artiklarna 21 och 23 i direktiv (EU) 2022/2555 eller den tillsyn och efterlevnadskontroll som fastställs i kapitel VII i enlighet med artikel 4.1 och 4.2 i det direktivet, och därför bör artiklarna 9 och 16 tillämpas i sin helhet på sektorer, även om det finns sektorsspecifika unionsrättsakter i den mening som avses i artikel 4, Följaktligen ska medlemsstaterna utse eller inrätta en eller flera cyberkrishanteringsmyndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser som inträffar i sektorer som omfattas av sektorsspecifika unionsrättsakter. Man ska inte heller underlåta att beakta sektorer som omfattas av sektorsspecifika unionsrättsakter när den nationella planen för hanteringen av storskaliga cybersäkerhetsincidenter och kriser antas. Slutligen ska EU-CyCLONe utföra sina uppgifter enligt artikel 16 i direktiv (EU) 2022/2555 med avseende på sektorer där entiteter omfattas av sektorsspecifika unionsrättsakter.

III.5. **Undantag från tillämpningen av artiklarna 3.3, 3.4, 20, 27.2 och 27.3.**

37. I enlighet med artikel 3.3 i direktiv (EU) 2022/2555 ska medlemsstaterna upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster som omfattas av det direktivet. I enlighet med artikel 27.2 ska medlemsstaterna ålägga de entiteter som avses i artikel 27.1 i det direktivet att lämna vissa uppgifter till de behöriga myndigheterna. Eftersom syftet med dessa bestämmelser är att säkerställa en tydlig överblick över de entiteter som omfattas av direktiv (EU) 2022/2555 för att stödja tillsynen över väsentliga och viktiga entiteter som omfattas av direktivets tillämpningsområde, ska dessa bestämmelser inte tillämpas på entiteter som omfattas av sektorsspecifika unionsrättsakter när det gäller riskhanteringsåtgärder för cybersäkerhet och rapporteringskrav. Detta hindrar inte att medlemsstaterna inkluderar sådana entiteter i förteckningen.

I enlighet med artikel 20.1 i direktiv (EU) 2022/2555 ska väsentliga och viktiga entiteters ledningsorgan godkänna de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, och de ska övervaka genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln. I enlighet med artikel 20.2 i det direktivet ska medlemsstaterna säkerställa att medlemmarna i väsentliga och viktiga entiteters ledningsorgan är skyldiga att genomgå utbildning, och ska uppmuntra väsentliga och viktiga entiteter att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten. Skyldigheterna enligt artikel 20 i direktiv (EU) 2022/2555 är direkt kopplade till kraven enligt artikel 21 i det direktivet, och följaktligen ska artikel 20 inte tillämpas när det finns sektorsspecifika unionsrättsakter i den mening som avses i artikel 4 i det direktivet som är tillämpliga på riskhanteringskrav för cybersäkerhet.

TILLÄGG

Sektorsspecifika unionsrättsakter

Förordning (EU) 2022/2554 (rättsakten om digital operativ motståndskraft) ([1])

1. I artikel 1.2 i förordning (EU) 2022/2554 (rättsakten om digital operativ motståndskraft) fastställs, när det gäller finansiella entiteter som omfattas av direktiv (EU) 2022/2555 och motsvarande nationella regler för införlivande av direktivet, att förordning (EU) 2022/2554 ska betraktas som en sektorsspecifik unionsrättsakt vid tillämpningen av artikel 4 i direktiv (EU) 2022/2555. Denna utsaga återspeglas i skäl 28 i direktiv (EU) 2022/2555, där det anges att rättsakten om digital operativ motståndskraft bör betraktas som en sektorsspecifik unionsrättsakt i förhållande till direktiv (EU) 2022/2555 när det gäller finansiella entiteter. Följaktligen ska bestämmelserna i förordning (EU) 2022/2554 avseende riskhanteringsåtgärder för informations- och kommunikationsteknik (IKT) (artikel 6 och följande), hantering av IKT-relaterade incidenter och i synnerhet rapportering om större IKT-relaterade incidenter (artikel 17 och följande), samt avseende testning av digital operativ motståndskraft (artikel 24 och följande), arrangemang för informationsutbyte (artikel 25) och IKT-tredjepartsrisk (artikel 28 och följande) tillämpas i stället för de bestämmelser som fastställs i detta direktiv. Medlemsstaterna ska därför inte tillämpa bestämmelserna i direktiv (EU) 2022/2555 om riskhanterings- och rapporteringsskyldigheter beträffande cybersäkerhet och om tillsyn och efterlevnadskontroll på finansiella entiteter som omfattas av förordning (EU) 2022/2554.

2. I detta hänseende betraktas finansiella entiteter som entiteter enligt artikel 2.1 a–t i förordning (EU) 2022/2554. De typer av entiteter som omfattas av förordning (EU) 2022/2554 såsom finansiella entiteter, och som även omfattas av direktiv (EU) 2022/2555 såsom väsentliga och viktiga entiteter, inbegriper kreditinstitut, handelsplatser och centrala motparter. I och med att det är viktigt att upprätthålla en stark förbindelse och ett informationsutbyte med finanssektorn inom ramen för direktiv (EU) 2022/2555, får de europeiska tillsynsmyndigheterna och de behöriga myndigheterna inom ramen för förordning (EU) 2022/2554 begära att delta i samarbetsgruppens verksamhet ([2]) och utbyta information och samarbeta med de gemensamma kontaktpunkterna och med CSIRT-enheterna och de behöriga myndigheterna inom ramen för direktiv (EU) 2022/2555 ([3]). De behöriga myndigheterna enligt förordning (EU) 2022/2554 bör även översända uppgifter om större IKT-relaterade incidenter och, i förekommande fall, betydande cyberhot till CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt direktiv (EU) 2022/2555. Man kan göra detta genom att ge omedelbar tillgång till incidentanmälningar och vidarebefordra dem antingen direkt eller genom en gemensam kontaktpunkt. CSIRT-enheterna bör kunna inbegripa finanssektorn i sin verksamhet ([4]). Medlemsstaterna bör fortsätta att inkludera finanssektorn i sina strategier för cybersäkerhet. Bestämmelserna om nationella ramar för hantering av cybersäkerhetskriser (artikel 9 i direktiv (EU) 2022/2555) och om EU-CyCLONe (artikel 16 i direktiv (EU) 2022/2555) ska även fortsättningsvis tillämpas på entiteter som omfattas av förordning (EU) 2022/2554.

([1]) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).

([2]) Artikel 14.3 i direktiv (EU) 2022/2555 och artikel 47.1 i förordning (EU) 2022/2554.

([3]) Se skäl 28 i direktiv (EU) 2022/2555.

([4]) Ibid.

IV

(Upplysningar)

UPPLYSNINGAR FRÅN EUROPEISKA UNIONENS INSTITUTIONER, BYRÅER OCH ORGAN

RÅDET

Meddelande till de personer och enheter som omfattas av de åtgärder som föreskrivs i rådets beslut 2011/235/Gusp, genomfört genom rådets genomförandebeslut (Gusp) 2023/1780, och i rådets förordning (EU) nr 359/2011, genomförd genom rådets genomförandeförordning (EU) 2023/1779, om restriktiva åtgärder mot vissa personer, enheter och organ med hänsyn till situationen i Iran

(2023/C 328/03)

Följande information lämnas för kännedom till de personer och enheter som anges i bilagan till rådets beslut 2011/235/Gusp ([1]), genomfört genom rådets genomförandebeslut (Gusp) 2023/1780 ([2]), och i bilaga I till rådets förordning (EU) nr 359/2011 ([3]), genomförd genom rådets genomförandeförordning (EU) 2023/1779 ([4]) om restriktiva åtgärder mot vissa personer, enheter och organ med hänsyn till situationen i Iran.

Europeiska unionens råd har beslutat att dessa personer och enheter bör ingå i förteckningen över personer och enheter som är föremål för restriktiva åtgärder enligt beslut 2011/235/Gusp och förordning (EU) nr 359/2011.

De berörda personerna och enheterna uppmärksammas på möjligheten att vända sig till de behöriga myndigheter i medlemsstaten/medlemsstaterna i fråga som anges på de webbplatser som förtecknas i bilaga II till förordning (EU) nr 359/2011 med en ansökan om tillstånd att få använda frysta tillgångar för grundläggande behov eller särskilda betalningar (jfr artikel 4 i förordningen).

De berörda personerna och enheterna kan före den 1 januari 2024 inkomma med en ansökan till rådet, åtföljd av styrkande handlingar, om att beslutet om att föra upp dem på den ovannämnda förteckningen ska omprövas. Ansökan ska skickas till följande adress:

Europeiska unionens råd
Generalsekretariatet
RELEX.1
Rue de la Loi 175/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-post: sanctions@consilium.europa.eu

([1]) EUT L 100, 14.4.2011, s. 51.
([2]) EUT L 228 I, 15.9.2023, s. 6.
([3]) EUT L 100, 14.4.2011, s. 1.
([4]) EUT L 228 I, 15.9.2023, s. 1.

De berörda personerna och enheterna uppmärksammas också på möjligheten att väcka talan mot rådets beslut vid Europeiska unionens tribunal i enlighet med villkoren i artiklarna 275 andra stycket och 263 fjärde och sjätte styckena i fördraget om Europeiska unionens funktionssätt.

Meddelande till de registrerade som omfattas av de restriktiva åtgärder som föreskrivs i rådets beslut 2011/235/Gusp och rådets förordning (EU) nr 359/2011 om restriktiva åtgärder mot vissa personer, enheter och organ med hänsyn till situationen i Iran

(2023/C 328/04)

De registrerade ombeds uppmärksamma följande information i enlighet med artikel 16 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([1]).

De rättsliga grunderna för denna behandling är rådets beslut 2011/235/Gusp ([2]), genomfört genom rådets genomförandebeslut (Gusp) 2023/1780 ([3]), och rådets förordning (EU) nr 359/2011 ([4]), genomförd genom rådets genomförandeförordning (EU) 2023/1779 ([5]).

Den personuppgiftsansvarige för denna behandling är Europeiska unionens råd, som företräds av generaldirektören för generaldirektoratet för yttre förbindelser (Relex) vid rådets generalsekretariat, och den avdelning som har anförtrotts behandlingen är direktoratet för övergripande och globala frågor (Relex.1), som kan kontaktas på följande adress:

Europeiska unionens råd
Generalsekretariatet
RELEX.1
Rue de la Loi 175/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-post: sanctions@consilium.europa.eu

Rådets dataskyddsombud kan kontaktas på följande e-postadress:

Dataskyddsombudet

data.protection@consilium.europa.eu

Syftet med behandlingen är att upprätta och uppdatera en förteckning över personer som är föremål för restriktiva åtgärder enligt beslut 2011/235/Gusp, genomfört genom rådets genomförandebeslut (Gusp) 2023/1780, och förordning (EU) nr 359/2011, genomförd genom rådets genomförandeförordning (EU) 2023/1779.

De registrerade är de fysiska personer som uppfyller kriterierna för uppförande på förteckningen enligt beslut 2011/235/Gusp och förordning (EU) nr 359/2011.

De personuppgifter som samlats in omfattar uppgifter som är nödvändiga för en korrekt identifiering av den berörda personen, motiveringen och andra uppgifter med koppling till skälen för uppförandet på förteckningen.

De rättsliga grunderna för hanteringen av personuppgifter är de rådsbeslut som antagits i enlighet med artikel 29 i EU-fördraget och de rådsförordningar som antagits i enlighet med artikel 215 i EUF-fördraget där fysiska personer (registrerade) förtecknas, tillgångar fryses och reserestriktioner införs.

Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse i enlighet med artikel 5.1 a och för att fullgöra sådana rättsliga förpliktelser som fastställs i de ovannämnda rättsakterna och som åvilar den personuppgiftsansvarige i enlighet med artikel 5.1 b i förordning (EU) 2018/1725.

Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse i enlighet med artikel 10.2 g i förordning (EU) 2018/1725.

Rådet får inhämta personuppgifter om registrerade från medlemsstaterna och/eller Europeiska utrikestjänsten. Mottagarna av personuppgifterna är medlemsstaterna, Europeiska kommissionen och Europeiska utrikestjänsten.

([1]) EUT L 295, 21.11.2018, s. 39.
([2]) EUT L 100, 14.4.2011, s. 51.
([3]) EUT L 228 I, 15.9.2023, s. 6.
([4]) EUT L 100, 14.4.2011, s. 1.
([5]) EUT L 228 I, 15.9.2023, s. 1.

Alla personuppgifter som behandlas av rådet inom ramen för autonoma EU-sanktioner kommer att bevaras i fem år från och med den dag då den registrerade har avförts från förteckningen över personer som är föremål för frysningen av tillgångar eller åtgärdens giltighetstid har löpt ut eller, om talan väcks vid domstolen, tills en slutlig dom har meddelats. Personuppgifter i handlingar som registrerats av rådet sparas av rådet för arkivändamål av allmänt intresse i den mening som avses i artikel 4.1 e i förordning (EU) 2018/1725.

Rådet kan behöva utbyta personuppgifter om en registrerad med ett tredjeland eller en internationell organisation i samband med rådets införlivande av uppföranden som FN gjort på sin förteckning eller inom ramen för internationellt samarbete när det gäller EU:s politik för restriktiva åtgärder.

I avsaknad av ett beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder grundar sig överföringen av personuppgifter till ett tredjeland eller en internationell organisation på följande villkor, i enlighet med artikel 50 i förordning (EU) 2018/1725: Överföringen är nödvändig av viktiga skäl som rör allmänintresset. Överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Inget automatiserat beslutsfattande ingår i behandlingen av den registrerades personuppgifter.

Registrerade har rätt till information och rätt att få tillgång till sina personuppgifter. De har också rätt att få sina uppgifter korrigerade och kompletterade. Under vissa omständigheter kan de även ha rätt att få sina personuppgifter raderade, att göra invändningar mot behandlingen av deras personuppgifter eller att begära att behandlingen ska begränsas.

De registrerade kan utöva dessa rättigheter genom att skicka ett e-postmeddelande till den personuppgiftsansvarige med en kopia till dataskyddsombudet på e-postadressen ovan.

De registrerade ska till sin begäran bifoga en kopia av en identitetshandling för att bekräfta sin identitet (id-kort eller pass). Denna handling ska innehålla ett identifikationsnummer, utfärdandeland, giltighetstid, namn, adress och födelsedatum. Andra uppgifter på identitetshandlingen, t.ex. foto eller personliga kännetecken, får döljas.

Registrerade har rätt att lämna in ett klagomål till Europeiska datatillsynsmannen i enlighet med förordning (EU) 2018/1725 (edps@edps.europa.eu).

Dessförinnan rekommenderas de registrerade att först försöka få problemet åtgärdat genom att kontakta den personuppgiftsansvarige och/eller rådets dataskyddsombud.

EUROPEISKA KOMMISSIONEN

Sammanfattning av Europeiska kommissionens beslut om tillstånd för utsläppande på marknaden för användningen och/eller för användning av de ämnen som förtecknas i bilaga XIV till Europaparlamentets och rådets förordning (EG) nr 1907/2006 om registrering, utvärdering, godkännande och begränsning av kemikalier (Reach)

(Offentliggjord i enlighet med artikel 64.9 i förordning (EG) nr 1907/2006 ([1]))

(Text av betydelse för EES)

(2023/C 328/05)

Beslut om återkallande av tillstånd

Hänvisning till beslutet ([1])	Datum för beslutet	Ämnesnamn	Mottagare av beslutet	Återkallad användning	Upphävt beslut	Skäl för beslutet
C(2023) 6014	11 september 2023	Natriumdikromat EG-nr: 234-190-3, CAS-nr: 10588-01-9 (vattenfri), CAS-nr: 7789-12-0 (dihydrat)	Gruppo Colle S.r.l., Via G. Di Vittorio 3/5, 59025 Usella, Cantagallo, Prato, Italien	Som betmedel vid färgning av ull med mörka färger	C(2017) 8331	Omprövningsrapporten påvisade inte att det saknas lämpliga alternativ för sökanden, i enlighet med artikel 60.4 i förordning (EG) nr 1907/2006.

([1]) Beslutet finns på Europeiska kommissionens webbplats: Authorisation (europa.eu).

([1]) EUT L 396, 30.12.2006, s. 1.

Eurons växelkurs [1]

15 september 2023

(2023/C 328/06)

1 euro =

	Valuta	Kurs		Valuta	Kurs
USD	US-dollar	1,0658	CAD	kanadensisk dollar	1,4409
JPY	japansk yen	157,50	HKD	Hongkongdollar	8,3416
DKK	dansk krona	7,4573	NZD	nyzeeländsk dollar	1,8008
GBP	pund sterling	0,85878	SGD	singaporiansk dollar	1,4524
SEK	svensk krona	11,8730	KRW	sydkoreansk won	1 415,78
CHF	schweizisk franc	0,9554	ZAR	sydafrikansk rand	20,2968
ISK	isländsk krona	145,30	CNY	kinesisk yuan renminbi	7,7561
NOK	norsk krona	11,4220	IDR	indonesisk rupiah	16 379,21
BGN	bulgarisk lev	1,9558	MYR	malaysisk ringgit	4,9922
CZK	tjeckisk koruna	24,496	PHP	filippinsk peso	60,612
HUF	ungersk forint	383,75	RUB	rysk rubel	
PLN	polsk zloty	4,6308	THB	thailändsk baht	38,145
RON	rumänsk leu	4,9698	BRL	brasiliansk real	5,1860
TRY	turkisk lira	28,7513	MXN	mexikansk peso	18,2275
AUD	australisk dollar	1,6498	INR	indisk rupie	88,6150

[1] *Källa:* Referensväxelkurs offentliggjord av Europeiska centralbanken.

V

(Yttranden)

FÖRFARANDEN FÖR GENOMFÖRANDE AV KONKURRENSPOLITIKEN

EUROPEISKA KOMMISSIONEN

Förhandsanmälan av en koncentration

(Ärende M.11239 – EDF / CREDIT MUTUEL / ILE-DE-FRANCE BUILDING)

Ärendet kan komma att handläggas enligt ett förenklat förfarande

(Text av betydelse för EES)

(2023/C 328/07)

1. Europeiska kommissionen mottog den 8 september 2023 en anmälan av en föreslagen koncentration i enlighet med artikel 4 i rådets förordning (EG) nr 139/2004 ([1]).

Denna anmälan berör följande företag:

— SAS C91 (Frankrike), kontrollerat av Électricité de France (*EDF*, Frankrike).

— La Française Real Estate Managers (*La Française*, Frankrike), kontrollerat av Caisse Régionale Crédit Mutuel Nord Europe (Frankrike), som i sin tur tillhör koncernen Crédit Mutuel (Frankrike).

— En fastighet i Ile-de-France (*byggnaden*, Frankrike).

EDF och Crédit Mutuel kommer att förvärva gemensam kontroll, på det sätt som avses i artikel 3.1 b i koncentrationsförordningen, över hela byggnaden.

Koncentrationen genomförs genom förvärv av tillgångar.

2. De berörda företagen bedriver följande affärsverksamhet:

— EDF: verksamt, i Frankrike och utomlands, inom produktion och grossistförsäljning av el, överföring, distribution och leverans av el, tillhandahållande av andra elrelaterade tjänster och, i mindre utsträckning, produktion och grossist- och detaljistförsäljning av gas.

— Crédit Mutuel: verksamt inom tillhandahållande av banktjänster och finansiella tjänster, främst i Frankrike. Genom sitt dotterbolag La Française erbjuder koncernen Crédit Mutuel fastighetsförvaltningstjänster.

3. Byggnaden är en kontors- och affärsbyggnad belägen på adressen 111, avenue de France, 75013 Paris, Frankrike.

4. Kommissionen har vid en preliminär granskning kommit fram till att den anmälda transaktionen kan omfattas av koncentrationsförordningen, dock med det förbehållet att ett slutligt beslut i denna fråga fattas senare.

([1]) EUT L 24, 29.1.2004, s. 1 (*koncentrationsförordningen*).

Det bör noteras att detta ärende kan komma att handläggas enligt ett förenklat förfarande, i enlighet med kommissionens tillkännagivande om ett förenklat förfarande för handläggning av vissa koncentrationer enligt rådets förordning (EG) nr 139/2004 ([2]).

5. Kommissionen uppmanar berörda tredje parter att till den lämna eventuella synpunkter på den föreslagna koncentrationen.

Synpunkterna ska ha kommit in till kommissionen senast tio dagar efter detta offentliggörande. Följande referens bör alltid anges:

M.11239 – EDF / CREDIT MUTUEL / ILE-DE-FRANCE BUILDING

Synpunkterna kan sändas till kommissionen per e-post eller per post. Använd följande kontaktuppgifter:

E-post: COMP-MERGER-REGISTRY@ec.europa.eu

Post:

Commission européenne
Direction générale de la concurrence
Greffe des concentrations
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

([2]) EUT C 366, 14.12.2013, s. 5.

ISSN 1977-1061 (elektronisk utgåva)
ISSN 1725-2504 (pappersutgåva)

Europeiska unionens
publikationsbyrå
L-2985 Luxemburg
LUXEMBURG

SV