EUROPEISKA CENTRALBANKENS BESLUT (EU) 2021/1486

av den 7 september 2021

om antagande av interna regler om begränsningar av registrerades rättigheter i samband med Europeiska centralbankens uppgifter som berör tillsynen över kreditinstitut (ECB/2021/42)

EUROPEISKA CENTRALBANKENS DIREKTION HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av stadgan för Europeiska centralbankssystemet och Europeiska centralbanken, särskilt artikel 11.6,

med beaktande av Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG ([1]), särskilt artikel 25, och

av följande skäl:

(1) Europeiska centralbanken (ECB) utför sina uppgifter i enlighet med fördragen och rådets förordning (EU) nr 1024/2013 ([2]).

(2) I enlighet med artikel 45.3 i Europaparlamentets och rådets förordning (EU) 2018/1725 fastställer Europeiska centralbankens beslut (EU) 2020/655 (ECB/2020/28) ([3]) de allmänna bestämmelserna som genomför förordning (EU) 2018/1725 vad gäller ECB. I synnerhet anges reglerna för utnämning av och rollen för dataskyddsombud (DPO) hos ECB, inbegripet dataskyddsombudets arbetsuppgifter, åligganden och befogenheter.

(3) Vid utövandet av de uppgifter som ECB tilldelats fungerar ECB, och särskilt den berörda organisatoriska enheten, som personuppgiftsansvarig när den, ensam eller tillsammans med andra, fastställer ändamålen och medlen för att behandla personuppgifter.

(4) Enligt artikel 4.1 i förordning (EU) nr 1024/2013 har ECB exklusiv befogenhet att för tillsynsändamål, i syfte att säkerställa kreditinstitutens säkerhet och sundhet och det finansiella systemets stabilitet, utföra specifika uppgifter i förhållande till alla kreditinstitut som är etablerade i de medlemsstater som deltar i den gemensamma tillsynsmekanismen (SSM).

(5) När ECB utför dessa specifika uppgifter behandlar den flera olika informationskategorier som kan hänföra sig till en identifierad eller identifierbar fysisk person som t.ex. identifieringsuppgifter, kontaktuppgifter, yrkesrelaterade, ekonomiska eller administrativa uppgifter, uppgifter från specifika källor, uppgifter om elektronisk kommunikation samt elektroniska trafikuppgifter, uppgifter ur kriminalregister, översikt över ekonomiska och icke-ekonomiska intressen, information om en persons eller dennes nära anhörigas relationer till enheter som står under tillsyn eller till ledamöter i ett ledningsorgan för enheter som står under tillsyn samt uppgifter om de tjänster som en person har utnämnts eller kan komma att utnämnas till. Personuppgifter kan också ingå som en del i en bedömning som görs i samband med auktorisationen av ett kreditinstitut, återkallandet av ett kreditinstituts auktorisation och förfaranden för kvalificerade innehav, etableringsrätten för en betydande enhet som står under tillsyn, bedömningen av huruvida lämplighetskrav uppfylls, de ersättningspolicyer som en betydande enhet som står under tillsyn tillämpar, krediter som en sådan enhet beviljar personer i ledande ställning inom företaget eller personer som har en anknytning till sådana personer, samt i samband med anklagelser om eventuella brott mot de rättsakter som avses i artikel 4.3 i förordning (EU) nr 1024/2013.

([1]) EUT L 295, 21.11.2018, s. 39.

([2]) Rådets förordning (EU) nr 1024/2013 av den 15 oktober 2013 om tilldelning av särskilda uppgifter till Europeiska centralbanken i fråga om politiken för tillsyn över kreditinstitut (EUT L 287, 29.10.2013, s. 63).

([3]) Europeiska centralbankens beslut (EU) 2020/655 av den 5 maj 2020 om antagande av genomförandebestämmelser om uppgiftsskydd vid Europeiska centralbanken och om upphävande av beslut ECB/2007/1 (ECB/2020/28) (EUT L 152, 15.5.2020, s. 13).

(6) När ECB utför dessa specifika uppgifter är målsättningen att uppnå unionens viktiga mål av generellt allmänt intresse. Av denna orsak bör utförandet av sådana uppgifter säkerställas enligt vad som diskuteras i förordning (EU) 2018/1725, särskilt artikel 25.1 c och g. När ECB utför sådana uppgifter arbetar den för unionens viktiga mål av generellt allmänt intresse, i egenskap av en myndighet som för tillsynsändamål ansvarar för att utföra specifika uppgifter i förhållande till alla kreditinstitut som är etablerade i de medlemsstater som deltar i SSM. Sådana uppgifter omfattar en tillsyns-, inspektions- eller regleringsfunktion som har ett samband med myndighetsutövning vid tillsynen över kreditinstitut.

(7) I detta sammanhang är det lämpligt att ange de grunder på vilka ECB får begränsa de registrerades rättigheter avseende uppgifter som erhållits när ECB utför sina tillsynsuppgifter enligt förordning (EU) nr 1024/2013.

(8) I enlighet med artikel 25.1 i förordning (EU) 2018/1725 bör begränsningar av tillämpningen av artiklarna 14–22, 35 och 36 och, i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som föreskrivs i artiklarna 14–22, artikel 4 i den förordningen fastställas i interna regler eller rättsakter som antas med stöd av fördragen. ECB bör därför fastställa de regler enligt vilka den får begränsa de registrerades rättigheter när den utför sina tillsynsuppgifter.

(9) I detta beslut fastställs regler för ECB:s begränsning av de registrerades rättigheter när den utför sina tillsynsuppgifter, men direktionen avser att anta ett separat beslut om interna regler om begränsningar av dessa rättigheter när ECB behandlar personuppgifter inom ramen för sin interna verksamhet.

(10) ECB kan eventuellt tillämpa ett undantag i enlighet med förordning (EU) 2018/1725 vilket gör en begränsning onödig, särskilt de som anges i artiklarna 15.4, 16.5, 19.3 och 35.3 i den förordningen. För behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål kan ECB eventuellt tillämpa ett undantag som anges i artikel 16.5 b eller artikel 19.3 d i förordning (EU) 2018/1725.

(11) Utövandet av de registrerades rättigheter enligt artiklarna 17, 18, 20, 21, 22 och 23 i förordning (EU) 2018/1725 kan göra det omöjligt eller allvarligt försvåra möjligheten att uppnå vissa mål, däribland arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Därför bör det här beslutet föreskriva ett undantag från dessa rättigheter i enlighet med artikel 25.3 eller 25.4 i förordning (EU) 2018/1725, med förbehåll för lämpliga skyddsåtgärder.

(12) ECB bör motivera varför sådana begränsningar av de registrerades rättigheter är absolut nödvändiga och proportionella i ett demokratiskt samhälle för att skydda de mål som eftersträvas vid utövandet av dess offentliga makt och de funktioner som är knutna till denna, samt hur ECB respekterar de grundläggande rättigheterna och friheterna samtidigt som sådana begränsningar införs.

(13) Inom denna ram är ECB skyldig att i största möjliga utsträckning respektera de registrerades grundläggande rättigheter, särskilt de som rör rätten till information, tillgång och rättelse, rätt till radering, begränsning av behandling, underrättelse om en personuppgiftsincident till den registrerade eller konfidentialitet för kommunikation enligt förordning (EU) 2018/1725.

(14) ECB kan dock vara skyldig att begränsa den information som lämnas till registrerade och registrerades rättigheter för att skydda utförandet av sina tillsynsuppgifter, särskilt sina egna utredningar och förfaranden, andra myndigheters utredningar och förfaranden samt andra personers grundläggande rättigheter och friheter i samband med ECB:s utredningar eller andra förfaranden.

(15) ECB bör häva en begränsning som redan har tillämpats i den utsträckning som den inte längre behövs.

(16) ECB:s dataskyddsombud bör granska tillämpningen av begränsningar för att säkerställa att detta beslut och förordning (EU) 2018/1725 följs.

(17) Europeiska datatillsynsmannen har hörts i enlighet med artikel 41.2 i förordning (EU) nr 2018/1725 och avgav ett yttrande den 12 mars 2021.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte och omfattning

1. I detta beslut fastställs regler för ECB:s begränsning av de registrerades rättigheter vid behandling av personuppgifter som registreras i det centrala registret i samband med att ECB utför sina tillsynsuppgifter enligt förordning (EU) nr 1024/2013.

2. De registrerades rättigheter som kan begränsas anges i följande artiklar i förordning (EU) 2018/1725:

a) Artikel 14 (klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter).

b) Artikel 15 (information som ska tillhandahållas när personuppgifter samlas in från den registrerade).

c) Artikel 16 (information som ska tillhandahållas om personuppgifter inte har erhållits från den registrerade).

d) Artikel 17 (den registrerades rätt till tillgång).

e) Artikel 18 (rätt till rättelse).

f) Artikel 19 (rätt till radering (”rätten att bli bortglömd”).

g) Artikel 20 (rätt till begränsning av behandling).

h) Artikel 21 (anmälningsskyldighet avseende rättelse eller radering av person–uppgifter och begränsning av behandling).

i) Artikel 22 (rätt till dataportabilitet).

j) Artikel 35 (information till den registrerade om en personuppgiftsincident).

k) Artikel 36 (konfidentialitet för elektronisk kommunikation).

l) Artikel 4 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som föreskrivs i artiklarna 14–22 i förordning (EU) 2018/1725.

Artikel 2

Definitioner

I detta beslut gäller följande definitioner:

1. *behandling*: behandling såsom detta definieras i artikel 3.3 i förordning (EU) 2018/1725.

2. *personuppgifter*: personuppgifter såsom dessa definieras i artikel 3.1 i förordning (EU) 2018/1725.

3. *den registrerade*: en identifierad eller identifierbar fysisk person, varvid en identifierbar person är en person som direkt eller indirekt kan identifieras, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

4. *centralt register*: den offentligt tillgängliga lagringsplats för all behandling av personuppgifter som utförs vid ECB, som förs av ECB:s dataskyddsombud och som avses i artikel 9 i beslut (EU) 2020/655 (ECB/2020/28).

5. *personuppgiftsansvarig*: ECB, och särskilt den behöriga organisatoriska enhet inom ECB som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter och ansvarar för behandlingen.

6. *unionsinstitutioner och unionsorgan*: unionsinstitutioner och unionsorgan enligt definitionen i artikel 3.10 i förordning (EU) 2018/1725.

Artikel 3

Tillämpning av begränsningar

1. Den personuppgiftsansvarige får begränsa de rättigheter som avses i artikel 1.2 för att skydda de intressen och mål som avses i artikel 25.1 i förordning (EU) 2018/1725, särskilt om utövandet av dessa rättigheter skulle äventyra eller på annat sätt negativt påverka

a) ECB:s utförande av sina tillsynsuppgifter enligt förordning (EU) nr 1024/2013, inklusive att tillsynssystemet fungerar väl,

b) kreditinstitutens säkerhet och sundhet och det finansiella systemets stabilitet inom unionen och inom varje medlemsstat,

c) en effektiv rapportering av överträdelser i enlighet med artikel 23 i förordning (EU) nr 1024/2013.

2. För att skydda de intressen och mål som avses i artikel 25.1 i förordning (EU) 2018/1725 får den personuppgiftsansvarige begränsa de rättigheter som avses i artikel 1.2 med avseende på personuppgifter som erhållits från andra unionsinstitutioner och unionsorgan och behöriga myndigheter i medlemsstaterna eller i tredjeland samt internationella organisationer, under någon av följande omständigheter:

a) Om utövandet av dessa rättigheter kan begränsas av andra unionsinstitutioner och unionsorgan från vilka personuppgifterna erhållits, på grundval av andra rättsakter som föreskrivs i artikel 25 i förordning (EU) 2018/1725 eller i enlighet med kapitel IX i den förordningen eller grundläggande rättsakter från andra unionsinstitutioner och unionsorgan.

b) Om utövandet av dessa rättigheter kan begränsas av de behöriga myndigheterna i de medlemsstater från vilka personuppgifterna erhållits, på grundval av de rättsakter som avses i artikel 23 i Europaparlamentets och rådets förordning (EU) 2016/679 ([4]) eller enligt nationella åtgärder som införlivar artiklarna 13.3, 15.3 eller 16.3 i Europaparlamentets och rådets direktiv (EU) 2016/680 ([5]).

c) Om utövandet av dessa rättigheter kan äventyra eller på annat sätt negativt påverka ECB:s samarbete med tredjeländer eller internationella organisationer från vilka informationen erhållits, vid utförandet av dess uppgifter, såvida inte ECB:s intresse av samarbete uppvägs av de registrerades intressen eller grundläggande rättigheter och friheter.

([4]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

([5]) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

3. Innan en begränsning tillämpas i de fall som avses i punkt 2 a och 2 b ska den personuppgiftsansvarige

a) ta del av överenskommelser som ingåtts med berörda unionsinstitutioner och unionsorgan eller medlemsstaternas behöriga myndigheter, och

b) samråda med relevanta unionsinstitutioner och unionsorgan eller med medlemsstaternas behöriga myndigheter, såvida det inte är uppenbart för den personuppgiftsansvarige att tillämpningen av denna begränsning föreskrivs i någon av de rättsakter eller åtgärder som avses i punkt 2 a och 2 b.

4. Den personuppgiftsansvarige får endast tillämpa en begränsning om den efter en bedömning i det enskilda fallet drar slutsatsen att begränsningen

a) är nödvändig och proportionell med hänsyn till riskerna för den registrerades rättigheter och friheter, och

b) sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna i ett demokratiskt samhälle.

5. Den personuppgiftsansvarige ska dokumentera sin bedömning i en intern skriftlig not som ska innehålla den rättsliga grunden, skälen till begränsningen, den registrerades rättigheter som begränsas, de registrerade som påverkas, begränsningens nödvändighet och proportionalitet samt begränsningens förväntade varaktighet.

6. Den personuppgiftsansvariges beslut om att begränsa en registrerads rättigheter enligt detta beslut ska fattas av chefen eller biträdande chef för det affärsområde inom vilket den huvudsakliga behandlingen av personuppgifterna har genomförts.

Artikel 4

Undantag

1. Vid behandling för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får den personuppgiftsansvarige tillämpa undantag i enlighet med artikel 25.3 i förordning (EU) 2018/1725. I detta syfte får den personuppgiftsansvarige avvika från de rättigheter som avses i artiklarna 17, 18, 20 och 23 i förordning (EU) 2018/1725 i enlighet med de villkor som föreskrivs i artikel 25.3 i den förordningen.

2. Vid behandling för arkivändamål av allmänt intresse får den personuppgiftsansvarige tillämpa undantag i enlighet med artikel 25.4 i förordning (EU) 2018/1725. I detta syfte får den personuppgiftsansvarige avvika från de rättigheter som avses i artiklarna 17, 18, 20, 21, 22 och 23 i förordning (EU) 2018/1725 i enlighet med de villkor som föreskrivs i artikel 25.4 i den förordningen.

3. Sådana undantag ska omfattas av lämpliga skyddsåtgärder i enlighet med artikel 13 i förordning (EU) 2018/1725 och artikel 8 i detta beslut.

Artikel 5

Tillhandahållande av allmän information om begränsningar

Den personuppgiftsansvarige ska tillhandahålla allmän information om potentiella begränsningar av registrerades rättigheter enligt följande:

a) Den personuppgiftsansvarige ska ange vilka rättigheter som får begränsas, skälen till en begränsning och hur lång begränsningen kan vara.

b) Den personuppgiftsansvarige ska inkludera den information som avses i led a i sina meddelanden om uppgiftsskydd, integritetsmeddelanden och register över behandlingar som utförts i enlighet med artikel 31 i förordning (EU) 2018/1725.

Artikel 6

Begränsning av registrerades rätt till tillgång, rätt till rättelse, rätt till radering eller begränsning av behandling

1. Om den personuppgiftsansvarige helt eller delvis begränsar rätten till tillgång, rätten till rättelse, rätten till radering respektive rätten till begränsning av behandling som avses i artiklarna 17, 18, 19.1 och 20.1 i förordning (EU) 2018/1725, ska den personuppgiftsansvarige, inom den tidsperiod som avses i artikel 11.5 i beslut (EU) 2020/655 (ECB/2020/28), i sitt skriftliga svar på en begäran, informera den berörda registrerade om den begränsning som har tillämpats, de huvudsakliga skälen för begränsningen och om möjligheten att lämna in ett klagomål till Europeiska datatillsynsmannen eller begära rättslig prövning vid Europeiska unionens domstol.

2. Den personuppgiftsansvarige ska spara sin bedömning i en intern skriftlig not i enlighet med artikel 3.5 och, i tillämpliga fall, de handlingar som innehåller de underliggande faktiska och rättsliga omständigheterna och på begäran göra dessa tillgängliga för Europeiska datatillsynsmannen.

3. Den personuppgiftsansvarige får skjuta upp, utelämna eller neka tillhandahållande av information om skälen till den begränsning som avses i punkt 1 så länge som tillhandahållandet av information skulle undergräva syftet med begränsningen. Så snart den personuppgiftsansvarige konstaterar att tillhandahållandet av informationen inte längre undergräver syftet med begränsningen ska den personuppgiftsansvarige tillhandahålla den registrerade informationen.

Artikel 7

Begränsningarnas längd

1. Den personuppgiftsansvarige ska häva en begränsning så snart de omständigheter som motiverade begränsningen inte längre föreligger.

2. Om den personuppgiftsansvarige upphäver en begränsning enligt punkt 1 ska den personuppgiftsansvarige omedelbart

a) om så inte redan skett, informera den registrerade om de huvudsakliga skälen som låg till grund för en begränsning,

b) underrätta den registrerade om hans eller hennes rätt att lämna in ett klagomål till Europeiska datatillsynsmannen eller begära rättslig prövning vid Europeiska unionens domstol,

c) bevilja den registrerade den rättighet som omfattades av den begränsning som har hävts.

3. Den personuppgiftsansvarige ska var sjätte månad ompröva behovet av att bibehålla en begränsning som tillämpas i enlighet med detta beslut och ska skriftligen dokumentera sin förnyade bedömning i en intern not.

Artikel 8

Skyddsåtgärder

ECB ska tillämpa organisatoriska och tekniska skyddsåtgärder enligt bilagan för att förhindra missbruk eller olaglig tillgång eller överföring.

Artikel 9

Dataskyddsombudets granskning

1. Om den personuppgiftsansvarige begränsar en registrerad persons rättigheter måste den personuppgiftsansvarige fortlöpande involvera dataskyddsombudet. Särskilt gäller följande:

a) Den personuppgiftsansvarige ska utan onödigt dröjsmål samråda med dataskyddsombudet.

b) På dataskyddsombudets begäran ska den personuppgiftsansvarige ge dataskyddsombudet tillgång till alla handlingar som innehåller underliggande faktiska och rättsliga omständigheter, inbegripet sin bedömning i den interna skriftliga noten som avses i artikel 3.5.

c) Den personuppgiftsansvarige ska dokumentera hur dataskyddsombudet involverats, inbegripet vilken information som delats, särskilt datumet för det första samrådet som avses i led a.

d) Dataskyddsombudet får begära att den personuppgiftsansvarige på nytt granskar begränsningen.

e) Den personuppgiftsansvarige ska utan onödigt dröjsmål, och under alla omständigheter innan en begränsning tillämpas, skriftligen informera dataskyddsombudet om resultatet av den förnyade granskningen.

2. Den personuppgiftsansvarige ska informera dataskyddsombudet när en begränsning har hävts.

Artikel 10

Ikraftträdande

Detta beslut träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Frankfurt am Main den 7 september 2021.

Christine LAGARDE
ECB:s ordförande

BILAGA

Organisatoriska och tekniska skyddsåtgärder vid ECB för att förhindra missbruk eller olaglig tillgång eller överföring omfattar:

a) När det gäller personer:

   i) Alla personer som har tillgång till icke-offentlig ECB-information ska känna till och tillämpa ECB:s sekretessregler och regler för hanteringen av sekretessbelagd information.

   ii) Ett förfarande som säkerställer att endast kontrollerade och behöriga personer har tillgång till ECB:s lokaler och dess icke-offentliga information.

   iii) Åtgärder för att öka IT- och informationssäkerheten samt den fysiska säkerheten.

   iv) Utbildning som regelbundet anordnas för personal och externa tjänsteleverantörer.

   v) ECB:s anställda omfattas av strikta regler om tystnadsplikt, som framgår av anställningsvillkoren för Europeiska centralbankens personal och Europeiska centralbankens personalföreskrifter, vars åsidosättande medför disciplinära åtgärder.

   vi) Regler och skyldigheter som styr externa tjänsteleverantörers eller entreprenörers tillgång till icke-offentlig ECB-information som anges i avtal.

   vii) Tillträdeskontroller, inbegripet säkerhetsindelning, som ska säkerställa att personers tillgång till icke-offentlig ECB-information antingen tillåts eller begränsas utifrån verksamhetens behov och säkerhetskrav.

b) När det gäller processer:

   i) Processer har införts för att säkerställa att genomförande, drift och underhåll av IT-applikationer som stöder ECB:s verksamhet sker på ett kontrollerat sätt.

   ii) Man använder IT-applikationer för ECB:s verksamhet som uppfyller ECB:s säkerhetsstandarder.

   iii) Man har ett heltäckande fysiskt säkerhetsprogram i drift som kontinuerligt bedömer säkerhetshot och omfattar fysiska säkerhetsåtgärder för att säkerställa en adekvat skyddsnivå.

c) När det gäller teknik:

   i) Alla elektroniska uppgifter som lagras i IT-applikationer uppfyller ECB:s säkerhetsstandarder och skyddas därmed mot obehörig åtkomst eller ändring.

   ii) IT-applikationer implementeras, drivs och underhålls på en säkerhetsnivå som motsvarar IT-applikationernas sekretess-, integritets- och tillgänglighetsbehov, vilka bygger på driftskonsekvensanalyser.

   iii) Säkerhetsnivån för IT-applikationer valideras regelbundet genom tekniska och icke-tekniska säkerhetsbedömningar.

   iv) Tillgången till icke-offentlig ECB-information beviljas i enlighet med principen om behovsprövad behörighet, och privilegierad tillgång är mycket begränsad och strängt kontrollerad.

   v) Kontroller genomförs för att upptäcka och följa upp faktiska och potentiella säkerhetsöverträdelser.