Styrelsens yttrande (art 70.1.s)

Yttrande 28/2018

om Europeiska kommissionens förslag till genomförandebeslut om adekvat skydd av personuppgifter i Japan

Antaget den 5 december 2018

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit detta yttrande

med beaktande av artikel 70.1 s i 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,

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37 till detta, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018,

med beaktande av artikel 12 och artikel 22 i arbetsordningen av den 25 maj 2018.

HÄRIGENOM FRAMFÖRS FÖLJANDE:

1 SAMMANFATTNING

1. Europeiska kommissionen godkände sitt förslag till genomförandebeslut om adekvat skydd av personuppgifter från Japan i enlighet med den allmänna dataskyddsförordningen (nedan kallad *GDPR*)[1] den 5 september 2018[2]. Efter detta inledde kommissionen förfarandet för dess formella antagande.

2. Den 25 september 2018 begärde Europeiska kommissionen ett yttrande från Europeiska dataskyddsstyrelsen[3]. Kommissionen uppmanades tillhandahålla Europeiska dataskyddsstyrelsen all nödvändig dokumentation beträffande detta land, inbegripet all relevant korrespondens med den japanska regeringen.

3. Mot bakgrund av diskussionerna med Europeiska dataskyddsstyrelsen har Europeiska kommissionen ändrat sitt förslag till beslut om adekvat skyddsnivå två gånger och skickade sin senaste version den 13 november 2018[4]. Europeiska dataskyddsstyrelsen har baserat sitt aktuella yttrande på den senaste versionen av förslaget till genomförandebeslut (nedan kallat *förslaget till beslut om adekvat skyddsnivå*).

4. Europeiska dataskyddsstyrelsens bedömning av den skyddsnivå som säkerställs genom kommissionens beslut om adekvat skyddsnivå har gjorts genom en granskning av själva beslutet samt på grundval av en analys av den dokumentation som gjorts tillgänglig[5] av kommissionen[6].

5. Vid sin bedömning har Europeiska dataskyddsstyrelsen fokuserat både på de kommersiella aspekterna av förslaget till beslut om adekvat skyddsnivå och på statens tillgång till personuppgifter som överförts från EU för ändamål som hänför sig till brottsbekämpning och nationell säkerhet, inbegripet de

[1] Europaparlamentets och rådets förordning (EU) nr 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.
[2] Se pressmeddelande http://europa.eu/rapid/press-release_IP-18-5433_en.htm.
[3] Enligt artikel 70.1 s GDPR.
[4] Se bilaga I till Europeiska dataskyddsstyrelsens yttrande för den uppdaterade versionen av förslaget till kommissionens genomförandebeslut.
[5] Europeiska dataskyddsstyrelsen har grundat sin analys på översättningar som tillhandahållits av de japanska myndigheterna och kontrollerats av Europeiska kommissionen.
[6] Se bilaga II till Europeiska dataskyddsstyrelsens yttrande för förteckningen över dokument som Europeiska kommissionen inte har tillhandahållit Europeiska dataskyddsstyrelsen.

rättsmedel som är tillgängliga för enskilda personer i EU. Europeiska dataskyddsstyrelsen har även bedömt huruvida de skyddsåtgärder som föreskrivs enligt den japanska rättsliga ramen har införts och är effektiva.

6. Europeiska dataskyddsstyrelsen har i huvudsak grundat denna bedömning på sin referensram för adekvat skyddsnivå[7] som antogs i februari 2018.

1.1 Konvergensområden

7. Europeiska dataskyddsstyrelsens huvuduppgift har varit att avge ett yttrande till Europeiska kommissionen om den skyddsnivå som enskilda personer åtnjuter enligt det japanska ramverket. Det är viktigt att påpeka att Europeiska dataskyddsstyrelsen inte förväntar sig att den japanska rättsliga ramen ska kopiera EU:s dataskyddslagstiftning.

8. Europeiska dataskyddsstyrelsen erinrar om att det enligt EU-domstolens rättspraxis samt artikel 45 GDPR krävs att tredjelandets lagstiftning anpassas till de väsentliga grundläggande principer som fastställs i GDPR för att det ska anses föreligga en adekvat skyddsnivå. På dataskyddsområdet noterar Europeiska dataskyddsstyrelsen vidare att det föreligger en anpassning mellan GDPR och det japanska regelverket inom viktiga områden med avseende på vissa centrala bestämmelser, såsom korrekthet och uppgiftsminimering, lagringsminimering, datasäkerhet, ändamålsbegränsning och en oberoende tillsynsmyndighet, kommissionen för skydd av personuppgifter (nedan kallad *PPC*).

9. Utöver vad som anförts ovan välkomnar Europeiska dataskyddsstyrelsen ansträngningarna från kommissionen och de japanska myndigheterna för att säkerställa att Japan tillhandahåller en skyddsnivå som är likvärdig med den i GDPR, särskilt genom att fylla ut luckorna mellan GDPR och det japanska ramverket för uppgiftsskydd genom att anta ytterligare tilläggsregler för PPC som endast är tillämpliga för personuppgifter som överförs från EU till Japan. Europeiska dataskyddsstyrelsen noterar till exempel att PPC har åtagit sig att behandla ytterligare kategorier av uppgifter som känsliga uppgifter (känsliga uppgifter enligt den japanska lagstiftningen omfattar varken sexuell läggning eller medlemskap i fackföreningar). Genom tilläggsreglerna säkerställs dessutom att den registrerades rättigheter är tillämpliga på alla personuppgifter som överförs från EU, oberoende av lagringstid (medan det enligt japansk lagstiftning föreskrivs att den registrerades rättigheter inte är tillämpliga på personuppgifter som ska raderas inom en period på sex månader).

10. Europeiska dataskyddsstyrelsen noterar också Europeiska kommissionens ansträngningar för att stärka beslutet om adekvat skyddsnivå som en reaktion på de farhågor som aktualiserats av Europeiska dataskyddsstyrelsen.

1.2 Allmänna utmaningar

11. Trots detta återstår vissa utmaningar och Europeiska dataskyddsstyrelsen föreslår att följande huvudområden ska stärkas och övervakas noga i det japanska systemet.

12. Den första utmaningen är att övervaka denna nya struktur för att uppnå adekvat skyddsnivå, vilken utgör en kombination av en befintlig rättslig ram och särskilda tilläggsregler, för att säkerställa att den utgör ett hållbart och tillförlitligt system som inte gör att det uppkommer **praktiska problem när det gäller den konkreta och effektiva efterlevnaden** från de japanska enheterna och PPC:s tillsyn av efterlevnaden.

13. För det andra noterar Europeiska dataskyddsstyrelsen de upprepade åtaganden och försäkringar som Europeiska kommissionen och de japanska myndigheterna har gjort när det gäller tilläggsreglernas

[7] WP254, Referensram för adekvat skyddsnivå, 6 februari 2018.

bindande och verkställbara karaktär, samtidigt som Europeiska kommissionen uppmanas att **kontinuerligt övervaka deras bindande natur och effektiva tillämpning i Japan**, eftersom deras rättsliga status är en väsentlig beståndsdel med avseende på den adekvata skyddsnivån mellan EU och Japan. När det gäller PPC-riktlinjerna skulle Europeiska dataskyddsstyrelsen välkomna klargöranden i förslaget till beslut om adekvat skyddsnivå när det gäller **deras bindande karaktär och uppmanar kommissionen att noggrant övervaka denna aspekt**[8].

1.3 Särskilda kommersiella aspekter

14. När det gäller de kommersiella aspekterna av förslaget till beslut om adekvat skydd mellan EU och Japan har Europeiska dataskyddsstyrelsen vissa specifika farhågor och skulle vilja begära klargöranden av vissa viktiga frågor.

1.3.1 Europeiska dataskyddsstyrelsens betänkligheter när det gäller viktiga principer för uppgiftsskydd

15. Europeiska dataskyddsstyrelsen välkomnar att tilläggsreglerna utesluter att personuppgifter som överförts från EU överförs vidare till ett tredjeland på grundval av det ekonomiska samarbetet i Asien och Stillahavsområdet (nedan kallat *APEC*) – gränsöverskridande regler för uppgiftsskydd (Cross Border Privacy Rules, nedan kallade *CBPR-bestämmelser*). Dessutom erkänner Europeiska dataskyddsstyrelsen att kommissionen i sitt nya förslag till beslut om adekvat skyddsnivå har åtagit sig att upphäva beslutet om adekvat skyddsnivå om ett fortsatt skydd inte längre är säkerställt för framtida överföringar.

16. Enligt den japanska lagstiftningen är en av de rättsliga grunderna för vidare överföring ett erkännande att ett tredjeland tillhandahåller en skyddsnivå som är likvärdig med den japanska. Den japanska bedömningen av om ett tredjeland tillhandahåller adekvat skydd förefaller dock inte omfatta de särskilda ”tilläggsregler” som förhandlats fram mellan kommissionen och PPC, vilka bara är tillämpliga på personuppgifter från EU för att tillhandahålla en skyddsnivå som är väsentligen likvärdig med den i GDPR. Av detta följer att personuppgifter från EU som överförs från Japan till ett annat tredjeland som inte anses ha en ram för uppgiftsskydd som är väsentligen likvärdig med GDPR inte längre nödvändigtvis kommer att omfattas av det särskilda skyddet för personuppgifter från EU på grundval av den adekvata japanska skyddsnivån.

17. **Det ska emellertid påpekas att vidareöverföringar av personuppgifter kan komma att äga rum till tredjeländer som blir föremål för ett senare japanskt beslut om adekvat skyddsnivå. Dessa tredjeländer kanske inte har varit föremål för någon tidigare bedömning eller slutsats om adekvat skyddsnivå från EU. I en sådan situation bör kommissionen ta över sin övervakande roll och se till att skyddsnivån för uppgifter från EU upprätthålls eller överväga att upphäva detta beslut om adekvat skyddsnivå.**

18. Dessutom hyser Europeiska dataskyddsstyrelsen oro när det gäller de registeransvarigas (näringsidkare som hanterar personuppgifter) **skyldigheter vad gäller samtycke och öppenhet**. Europeiska dataskyddsstyrelsen har noggrant kontrollerat dessa aspekter eftersom användningen av samtycke som grund för behandling och för överföringar har en central roll i det japanska rättssystemet, något som inte är fallet i EU:s dataskyddslagstiftning. Exempelvis hyser Europeiska dataskyddsstyrelsen betänkligheter när det gäller begreppet samtycke som är definierat på ett sätt som inte omfattar ångerrätten, vilken är en väsentlig beståndsdel i EU:s lagstiftning för att säkerställa att den registrerade har verklig kontroll över sina personuppgifter. Med avseende på

[8] Se avsnitt 1.3.4 i detta yttrande för mer information.

transparenskraven för en näringsidkare som hanterar personuppgifter är det osäkert om den registrerade erhåller proaktiv information.

19. Europeiska dataskyddsstyrelsen är orolig för att det **japanska systemet för prövning** kan vara svårtillgängligt för personer i EU som behöver stöd eller vill inge klagomål mot bakgrund av det faktum att PPC:s stöd är tillgängligt via en telefontjänst och endast på japanska. Samma sak gäller för den medlingstjänst som PPC tillhandahåller, eftersom systemet inte har offentliggjorts på den engelskspråkiga versionen av PPC:s webbplats, medan viktiga informationsdokument, såsom de vanligaste frågorna om den japanska lagen om skydd av personuppgifter, också enbart är tillgängliga på japanska. I detta avseende skulle Europeiska dataskyddsstyrelsen välkomna om kommissionen och PPC kunde diskutera möjligheten att inrätta en onlinetjänst, åtminstone på engelska, i syfte att ge stöd till och hantera klagomål från enskilda personer i EU – liknande den som beskrivs i bilaga II till detta beslut om adekvat skyddsnivå. Det krävs även att kommissionen noga övervakar hur effektiva sanktionerna och de relevanta åtgärderna är.

1.3.2 Behov av förtydligande

20. Europeiska dataskyddsstyrelsen skulle välkomna försäkringar avseende vissa aspekter av förslaget till beslut om adekvat skyddsnivå som fortfarande kräver ytterligare klargöranden.

21. Dessa hänför sig exempelvis till vissa centrala begrepp i den japanska lagstiftningen. Närmare bestämt saknas det klarhet kring vilken **status den så kallade ”förvaltaren”** ska anses ha – ett begrepp som liknar personuppgiftsbiträdet enligt GDPR, men vars förmåga att fastställa och ändra ändamålen och medlen för behandlingen av personuppgifter fortfarande är oklar.

22. På grund av bristen på relevanta dokument skulle Europeiska dataskyddsstyrelsen även behöva försäkringar om huruvida **begränsningarna av enskilda personers rättigheter** (i synnerhet rätten till tillgång, rättelse och invändningar) är nödvändiga och proportionerliga i ett demokratiskt samhälle och om dessa respekterar grundprincipen bakom de grundläggande rättigheterna.

23. Europeiska dataskyddsstyrelsen förväntar sig också att Europeiska kommissionen noga övervakar det effektiva skyddet för **personuppgifter som överförs från EU till Japan, på grundval av förslaget till beslut om adekvat skyddsnivå, under hela deras ”livscykel”**, även om det i japansk lagstiftning endast föreskrivs en skyldighet att registrera uppgifternas ursprung i högst tre år.

1.4 Offentliga myndigheters tillgång till uppgifter som överförts till Japan

24. Europeiska dataskyddsstyrelsen har också analyserat den rättsliga ram som är tillämplig när japanska statliga enheter får tillgång till personuppgifter som överförs från EU till Japan för brottsbekämpande eller nationella säkerhetsändamål. Europeiska dataskyddsstyrelsen erkänner de garantier som den japanska regeringen har tillhandahållit, till vilka hänvisas som bilaga II till förslaget till beslut om adekvat skyddsnivå, men har identifierat ett antal aspekter som oroar och som kräver förtydligande, av vilka följande bör lyftas fram:

25. När det gäller brottsbekämpning noterar Europeiska dataskyddsstyrelsen att de rättsliga principer som är tillämpliga på tillgång till uppgifter ofta verkar likna reglerna i EU, i den mån de är tillgängliga. Avsaknaden av tillgängliga översättningar av flera lagtexter och relevant rättspraxis gör det dock svårt att fastställa att alla förfaranden för tillgång till uppgifter är nödvändiga och proportionerliga och att tillämpningen av dessa principer tillämpas på ett sätt som är ”väsentligen likvärdigt” med EU-lagstiftningen.

26. På området för nationell säkerhet erkänner Europeiska dataskyddsstyrelsen att den japanska regeringen har bekräftat att information endast kan erhållas från fritt tillgängliga källor eller genom

frivilligt utlämnande av uppgifter från företag, och att den inte samlar in information om allmänheten. Europeiska dataskyddsstyrelsen är dock medveten om de farhågor som uttryckts av experter och i medierna, och skulle välkomna ytterligare klargöranden om övervakningsåtgärder som vidtas av japanska statliga enheter.

27. När det gäller möjligheterna till rättslig prövning för enskilda personer i EU, inom området för brottsbekämpning samt nationell säkerhet, välkomnar Europeiska dataskyddsstyrelsen att Europeiska kommissionen och den japanska regeringen har förhandlat fram en ytterligare mekanism för att ge enskilda personer i EU en ytterligare möjlighet till prövning, och därigenom utvidga den japanska dataskyddsmyndighetens befogenheter. Det är dock fortfarande oroande att denna nya mekanism inte helt uppväger brister vad gäller tillsyn och prövning enligt japansk lagstiftning. Europeiska dataskyddsstyrelsen efterfrågar därför ytterligare klargöranden för att säkerställa att denna nya mekanism fullständigt kompenserar dessa brister.

1.5 Slutsats

28. Europeiska dataskyddsstyrelsen anser att detta beslut om adekvat skyddsnivå är av yttersta vikt. Eftersom det är det första beslutet om adekvat skyddsnivå sedan GDPR trädde i kraft kommer det att utgöra **ett prejudikat för framtida ansökningar om adekvat skyddsnivå samt för översynen av beslut om adekvat skyddsnivå som antagits enligt direktiv 95/46**[9]. Det är också viktigt att understryka att enskilda personer blir alltmer medvetna om globaliseringens inverkan på deras personliga integritet och vänder sig till sina tillsynsmyndigheter för att säkerställa att det finns tillräckliga garantier när deras personuppgifter överförs utomlands. Mot denna bakgrund anser Europeiska dataskyddsstyrelsen att kommissionen bör se till att det inte finns några brister i det skydd som beslutet om adekvat skyddsnivå mellan EU och Japan erbjuder och att denna specifika typ av adekvat skyddsnivå är anpassad till kraven i artikel 45 GDPR.

29. Europeiska dataskyddsstyrelsen välkomnar de ansträngningar som Europeiska kommissionen och den japanska PPC har gjort för att i så stor utsträckning som möjligt anpassa den japanska rättsliga ramen till EU:s. De **förbättringar** som införts genom tilläggsreglerna för att överbrygga några av skillnaderna mellan de två ramverken är mycket viktiga och välkomnas.

30. Efter en noggrann analys av kommissionens förslag till beslut om adekvat skyddsnivå och den japanska dataskyddsramen konstaterar Europeiska dataskyddsstyrelsen emellertid att **ett antal farhågor kvarstår, liksom ett behov av ytterligare klargöranden.** Denna särskilda typ av adekvat skyddsnivå där ett befintligt nationellt ramverk kombineras med ytterligare specifika regler medför även att det uppkommer frågor avseende dess operativa genomförande. Mot bakgrund av ovanstående rekommenderar Europeiska dataskyddsstyrelsen Europeiska kommissionen att behandla de farhågor och krav på klargöranden som Europeiska dataskyddsstyrelsen har tagit upp och tillhandahålla ytterligare bevisning och förklaringar avseende dessa frågor. Europeiska dataskyddsstyrelsen uppmanar också Europeiska kommissionen att se över denna slutsats om adekvat skyddsnivå (åtminstone) vartannat år och inte vart fjärde år såsom föreslås i det aktuella förslaget till beslut om adekvat skyddsnivå.

[9] 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.

2 INLEDNING

2.1 Japans ramverk för uppgiftsskydd

31. Japans ramverk för uppgiftsskydd moderniserades helt nyligen under 2017. Detta ramverk omfattar flera pelare och en central allmän lag, lagen om skydd av personuppgifter (nedan kallad *personuppgiftslagen*). En annan viktig rättsakt är det regeringsdekret som har i syfte att genomföra personuppgiftslagen (nedan kallat *regeringsdekretet*), i vilket vissa centrala principer i personuppgiftslagen specificeras.

32. På grundval av ett regeringsbeslut som antogs den 12 juni 2018[10] och artikel 6 i personuppgiftslagen erhöll PPC befogenhet att ”vidta nödvändiga åtgärder för att överbrygga skillnaderna i system och transaktioner mellan Japan och det berörda utländska landet i syfte att säkerställa lämplig hantering av de personuppgifter som erhållits från varje land”[11]. Regeringsbeslutet talar även för att de regler som PPC antagit som kompletterar eller går utöver dem som fastställts i personuppgiftslagen skulle vara bindande och verkställbara gentemot japanska näringsidkare[12].

33. Mot denna bakgrund inledde PPC förhandlingarna med Europeiska kommissionen och antog i juni 2018 strängare regler än dem i personuppgiftslagen och regeringsdekretet, vilka ska tillämpas på uppgifter som överförts från EU. Det är fråga om tilläggsregler enligt lagen om skydd av personuppgifter för hantering av personuppgifter som överförs från EU på grundval av ett beslut om adekvat skyddsnivå (nedan kallade *tilläggsreglerna*)[13]. Dessa tilläggsregler bifogas också som bilaga till förslaget till kommissionens genomförandebeslut som offentliggjordes i juli 2018.

34. Det är viktigt att notera att tilläggsreglerna endast är tillämpliga på personuppgifter som överförs från Europeiska unionen till Japan på grundval av beslutet om adekvat skyddsnivå och har i syfte att förbättra det tillämpliga skyddet för dessa uppgifter. Därför är dessa regler inte i sig tillämpliga på personuppgifter från enskilda i Japan eller som kommer från andra länder än de som tillhör EES.

35. Europeiska dataskyddsstyrelsen vill även uppmärksamma att den ändrade personuppgiftslagen trädde i kraft den 30 maj 2017 och att PPC i dess nuvarande form inrättades 2016. Dessutom har de tilläggsregler som PPC har förhandlat fram med Europeiska kommissionen ännu inte trätt i kraft, eftersom detta beror på om Europeiska kommissionen erkänner Japan som en jurisdiktion som är likvärdig med EU:s.

2.2 Omfattningen av Europeiska dataskyddsstyrelsens bedömning

36. Kommissionens förslag till beslut om adekvat skyddsnivå är resultatet av en bedömning av de japanska bestämmelserna om uppgiftsskydd, följt av förhandlingar med de japanska myndigheterna. Resultatet av dessa förhandlingar återspeglas särskilt i de två bilagor som bifogas förslaget till beslut om adekvat skyddsnivå: den första tillhandahåller ytterligare skydd som japanska näringsidkare är skyldiga att tillämpa vid behandling av personuppgifter som överförs från EU, medan den andra innehåller

[10] Europeiska dataskyddsstyrelsen noterar att enligt förslaget till beslut om adekvat skyddsnivå antogs detta regeringsbeslut den 12 juni 2018. Myndigheten erhöll dock endast ett utkast till regeringsbeslutet, vilket var daterat i april 2018.

[11] Regeringsbeslut av den 25 april 2018.

[12] Se avsnitt 1.3.4 nedan för mer information.

[13] Tilläggsregler, bilaga I till kommissionens genomförandebeslut av den XXXX, i enlighet med Europaparlamentets och rådets förordning 2016/679 om ett adekvat skydd av personuppgifter i Japan, som skickades till Europeiska dataskyddsstyrelsen i september 2018.

försäkringar och åtaganden från den japanska regeringen avseende tillgång till uppgifter från offentliga myndigheter.

37. Europeiska dataskyddsstyrelsen har granskat den japanska ramen för uppgiftsskydd, de tilläggsregler som förhandlats fram av Europeiska kommissionen och den japanska regeringens försäkringar och åtaganden. Europeiska dataskyddsstyrelsen förväntas avge ett oberoende yttrande om kommissionens bedömningar, identifiera eventuella brister i den rättsliga ramen för adekvat skyddsnivå och sträva efter att föreslå förändringar eller tillägg för att åtgärda dessa.

38. Såsom anges i Europeiska dataskyddsstyrelsens referensram för adekvat skyddsnivå bör ”informationen som lämnas av kommissionen vara uttömmande och göra det möjligt för Europeiska dataskyddsstyrelsen att göra en egen bedömning av skyddsnivån för uppgifter i tredjelandet”[14].

39. De flesta dokument som utgör en viktig del av det japanska rättssystemet, till vilka hänvisas i förslaget till beslut om adekvat skyddsnivå, har Europeiska dataskyddsstyrelsen emellertid erhållit i engelsk översättning. Europeiska dataskyddsstyrelsen avger därför detta yttrande på grundval av en analys av de dokument som är tillgängliga på engelska. Europeiska dataskyddsstyrelsen har beaktat den tillämpliga ramen för uppgiftsskydd i Europeiska unionen, inbegripet artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (nedan kallad *Europakonventionen*) som skyddar rätten till privat- och familjeliv samt artiklarna 7, 8 och 47 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) som skyddar rätten till privatliv och familjeliv, rätten till skydd av personuppgifter och rätten till ett effektivt rättsmedel och till en rättvis rättegång. Utöver detta har Europeiska dataskyddsstyrelsen beaktat kraven i GDPR samt relevant rättspraxis.

40. Syftet med denna översyn är att säkerställa att den japanska ramen för uppgiftsskydd är väsentligen likvärdig med den i Europeiska unionen. Begreppet ”adekvat skyddsnivå”, som redan fanns i direktiv 95/46, har vidareutvecklats av EU-domstolen. Det är viktigt att erinra om den standard som EU-domstolen fastställt i domen i målet Schrems, nämligen att ”skyddsnivån” i det tredje landet måste vara ”väsentligen likvärdig” med den som garanteras i EU, medan ”de medel som detta tredjeland använder för att säkerställa en sådan skyddsnivå kan skilja sig från dem som används inom [EU]”[15]. Syftet är därför inte att EU-lagstiftningen ska återspeglas punkt för punkt, utan att fastställa de grundläggande och centrala kraven i den lagstiftning som är föremål för undersökning. Adekvat skyddsnivå kan uppnås genom en kombination av rättigheter för de registrerade och skyldigheter för dem som behandlar data, eller som utövar kontroll över sådan behandling och tillsyn genom oberoende organ. Bestämmelserna om uppgiftsskydd är emellertid endast effektiva om de är verkställbara och följs i praktiken. Det är därför nödvändigt att inte bara beakta innehållet i de regler som är tillämpliga på personuppgifter som överförs till ett tredjeland eller en internationell organisation, utan även det system som finns för att säkerställa att sådana regler är effektiva. Effektiva tillsynsmekanismer är av yttersta vikt för att reglerna för uppgiftsskydd ska vara effektiva[16].

2.3 Allmänna synpunkter och farhågor

2.3.1 Särdrag som är kännetecknande för denna typ av beslut om adekvat skyddsnivå

41. Avtalet om adekvat skyddsnivå mellan EU och Japan är det första som granskas mot den nya rättsliga bakgrund som följer av GDPR. Detta innebär att Europeiska dataskyddsstyrelsens arbete blir allt

[14] WP254, s. 3.
[15] Domstolens dom av den 6 oktober 2015 i mål C-362/14, Maximillian Schrems/Data Protection Commissioner (punkterna 73 och 74).
[16] WP254, s. 2.

viktigare mot bakgrund av de effekter som detta förslag till beslut om adekvat skyddsnivå medför vid framtida ansökningar om adekvat skyddsnivå.

42. Avtalet om adekvat skyddsnivå mellan EU och Japan är också det första ömsesidiga avtalet. När och om EU erkänner att Japan tillhandahåller en skyddsnivå som är väsentligen likvärdig med den i GDPR, kommer Japan också att anta ett eget beslut om adekvat skyddsnivå enligt artikel 24 i personuppgiftslagen, och erkänna att EU tillhandahåller en adekvat skyddsnivå enligt den japanska ramen för uppgiftsskydd. Detta planerade avtal om adekvat skyddsnivå mellan Japan och EU har således en särskild karaktär, vilket Europeiska dataskyddsstyrelsen har beaktat vid sin bedömning. Såsom angetts ovan har den japanska PPC förhandlat fram specifika, striktare bestämmelser med Europeiska kommissionen, vilka endast är tillämpliga på personuppgifter som överförs från EU. Dessa striktare bestämmelser är bindande och verkställbara i enlighet med regeringsbeslutet och ska iakttas av alla de näringsidkare som hanterar personuppgifter i Japan vid behandlingen av personuppgifter som kommer från EU i enlighet med detta förslag till beslut om adekvat skyddsnivå.

43. Europeiska kommissionen har därför grundat sin bedömning om adekvat skyddsnivå både på det befintliga allmänna japanska ramverket för uppgiftsskydd och på dessa särskilda regler. Det faktum att det krävdes tilläggsregler för att komplettera personuppgiftslagen är ett tecken på att kommissionen erkänner att den japanska dataskyddslagstiftningen i sig inte är väsentligen likvärdig med GDPR.

44. **Mot bakgrund av de frågor som angetts ovan uppmanar Europeiska dataskyddsstyrelsen Europeiska kommissionen att se till att denna nya struktur för adekvat skyddsnivå, vilken är den första som antas enligt GDPR, som förlitar sig på tilläggsregler, utgör ett hållbart och tillförlitligt system som inte ger upphov till några praktiska problem med avseende på den konkreta och effektiva efterlevnaden från de japanska enheterna och kontrollen av efterlevnaden från PPC.**

2.3.2 Översättningarnas tillförlitlighet

45. I likhet med Europeiska kommissionen har Europeiska dataskyddsstyrelsen gjort sin bedömning på grundval av engelska översättningar som tillhandahållits av de japanska myndigheterna[17]. Europeiska dataskyddsstyrelsen uppmanar kommissionen att klargöra att den har baserat sitt förslag till beslut om adekvat skyddsnivå på de engelska översättningar som erhållits och regelbundet kontrollera kvaliteten på och tillförlitligheten hos dessa översättningar.

2.3.3 Sektorsspecifik adekvat skyddsnivå

46. I detta förslag till beslut om adekvat skyddsnivå är skyddet av personuppgifter begränsat till näringsidkare som hanterar personuppgifter i den mening som avses i personuppgiftslagen. Detta innebär att likvärdigheten är sektorsspecifik, eftersom den endast gäller den privata sektorn, och överföringar av personuppgifter mellan offentliga myndigheter och organ är undantagna. För närvarande anger kommissionen kortfattat detta särdrag vad gäller omfattningen av den adekvata skyddsnivån i skäl 10 i förslaget till beslut om adekvat skyddsnivå.

47. **Europeiska dataskyddsstyrelsen uppmanar kommissionen att i enlighet med artikel 45.3 GDPR uttryckligen ange den sektorsspecifika karaktären från detta beslut om adekvat skyddsnivå i genomförandebeslutets titel samt i artikel 1.**

2.3.4 Tilläggsreglernas och PPC-riktlinjernas bindande natur

48. I artikel 6 i personuppgiftslagen anges att ”regeringen ska ... vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att kunna vidta diskretionära åtgärder för att skydda personuppgifter vars korrekta hantering kräver ett särskilt strikt genomförande för att uppnå ett förstärkt skydd för en

[17] Europeiska kommissionen har kontrollerat dessa översättningar.

enskilds rättigheter och intressen, och ska vidta nödvändiga åtgärder i samarbete med regeringar i andra länder för att bygga upp ett internationellt formbart system beträffande personuppgifter genom att främja samarbete med en internationell organisation och andra internationella ramar." Även om det tydligt framgår av denna artikel i personuppgiftslagen att regeringen är behörig att vidta sådana rättsliga åtgärder, finns det inte någon direkt hänvisning att PPC är det organ som är behörigt att anta särskilda regler.[18] På grund av tidsbrist kunde Europeiska dataskyddsstyrelsen inte samla in, kontrollera och granska befintlig bevisning i detta hänseende.

49. **Mot bakgrund av betydelsen från denna fråga noterar Europeiska dataskyddsstyrelsen kommissionens och de japanska myndigheternas upprepade åtaganden och försäkringar beträffande tilläggsreglernas bindande och verkställbara karaktär. Europeiska dataskyddsstyrelsen uppmanar kommissionen att kontinuerligt övervaka att deras bindande natur och effektiva tillämpning i Japan, eftersom deras rättsliga status utgör en väsentlig beståndsdel av den adekvata skyddsnivån mellan Japan och EU.**

50. Dessutom hänvisar kommissionen i flera avsnitt i sitt förslag till beslut om adekvat skydd till PPC-riktlinjerna (nedan kallade *riktlinjerna*).

51. Även om kommissionen i skäl 16 i sitt förslag till beslut om adekvat skyddsnivå förtydligar att riktlinjerna ger en auktoritativ tolkning av personuppgiftslagen, anges det i samma skäl att dessa riktlinjer är bindande: "Enligt den information som mottagits från PPC betraktas dessa riktlinjer som bindande regler som utgör en integrerad del av den rättsliga ramen och som ska läsas tillsammans med texten i personuppgiftslagen, regeringsdekretet, genomförandebestämmelserna till personuppgiftslagen och en samling frågor och svar som PPC förberett."[19]

52. Europeiska dataskyddsstyrelsen gör emellertid, på grundval av samma information som tillhandahållits av PPC, bedömningen att riktlinjerna inte är rättsligt bindande. De kan snarare anses ge en "auktoritativ tolkning" av lagen. PPC hävdar att de näringsidkare som hanterar personuppgifter i praktiken följer riktlinjerna och att PPC använder dem för tillsynen av efterlevnaden av lagstiftningen från de näringsidkare som hanterar personuppgifter samt att domstolarna använder dem när de avkunnar sina domar. Dessa kriterier utgör dock inte tillräcklig bevisning för att riktlinjerna utgör rättsligt bindande normer.

53. **Europeiska dataskyddsstyrelsen välkomna förtydliganden i beslutet om adekvat skyddsnivå avseende PPC-riktlinjernas bindande karaktär och uppmanar kommissionen att noggrant övervaka denna aspekt.**

54. Enligt PPC följs riktlinjerna i praktiken, eftersom det är frågan om lokal sedvänja. PPC uppger att de japanska domstolarna använder sig av PPC-riktlinjerna för att avkunna sina domar vid tillämpningen av bestämmelserna i personuppgiftslagen. Kommissionen hänvisar till ett domstolsbeslut[20] från 2006

[18] Enligt en artikel som offentliggjordes i juli 2018, när ett utkast till tilläggsreglerna hade offentliggjorts, skulle den rättsligt bindande karaktären från dessa regler sannolikt bli föremål för en intern debatt i landet. Se Fujiwara S., Comparison between the EU and Japan's Data Protection Legal Frameworks', Jurist, vol. 1521 (juli 2018), s. 19.

[19] Kommissionens genomförandebeslut av den XXXX, i enlighet med Europaparlamentets och rådets förordning 2016/679 om ett adekvat skydd av personuppgifter i Japan, som skickades till Europeiska dataskyddsstyrelsen den 13 november 2018, skäl 16.

[20] Kommissionens genomförandebeslut av den XXXX, i enlighet med Europaparlamentets och rådets förordning 2016/679 om ett adekvat skydd av personuppgifter i Japan, som skickades till Europeiska dataskyddsstyrelsen den 13 november 2018, sidan 5, fotnot 16, "underrätten i Osaka, beslut av den 19 maj 2006, Hanrei Jiho, vol. 1948, s. 122".

som styrker att de japanska domstolarna stödjer sig på riktlinjerna vid sina avgöranden. Trots att Europeiska dataskyddsstyrelsen inte har erhållit denna dom skulle myndigheten uppskatta om kommissionen kunde tillhandahålla en mer aktuell dom, om en sådan finns tillgänglig, antingen inom området för dataskydd eller på ett annat område där de japanska domstolarna har använt PPC-riktlinjerna eller andra liknande riktlinjer som grund för sina domar.

2.3.5 Regelbunden översyn av beslutet om adekvat skyddsnivå

55. Enligt artikel 45.3 i GDPR ska en regelbunden översyn äga rum minst vart fjärde år. Enligt Europeiska dataskyddsstyrelsens referensram för adekvat skyddsnivå[21] ska detta betraktas som en generell tidsram som måste anpassas för varje tredjeland eller internationell organisation som omfattas av ett beslut om adekvat skyddsnivå. Beroende på de specifika omständigheter som råder kan det krävas att översynen utförs med tätare intervall. Dessutom kan incidenter eller annan information om eller ändringar i den rättsliga ramen för tredjelandet eller den internationella organisationen i fråga vara grund för att utföra en översyn tidigare än planerat. Det förefaller även lämpligt att ha en första översyn av ett helt nytt beslut om adekvat skyddsnivå relativt tidigt, och att sedan gradvis justera översynsintervallen utifrån resultatet.

56. Med beaktande av ett antal faktorer, bland annat det faktum att personuppgiftslagen trädde i kraft 2017, att PPC inrättades 2016 och att det ännu varken finns någon information eller någon bevisning beträffande den praktiska tillämpningen av tilläggsreglerna, **uppmanar Europeiska dataskyddsstyrelsen kommissionen att se över detta beslut om adekvat skyddsnivå (åtminstone) vartannat år och inte vart fjärde år som föreslås i det aktuella förslaget till beslut om adekvat skyddsnivå.**

2.3.6 Japans internationella åtaganden

57. I enlighet med artikel 45.2 c GDPR och referensramen för adekvat skyddsnivå[22], ska kommissionen, när den bedömer om skyddsnivån i ett tredjeland är tillräcklig, bland annat beakta vilka internationella åtaganden tredjelandet har gjort, eller andra skyldigheter som följer av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter, samt genomförandet av sådana skyldigheter. Dessutom bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk behandling av personuppgifter (nedan kallad *konvention 108+*)[23] och dess tilläggsprotokoll beaktas.

58. **I detta avseende noterar Europeiska dataskyddsstyrelsen att Japan är observatör i den rådgivande kommittén för konvention 108+.**

2.3.7 Dataskyddsmyndigheternas[24] befogenheter att väcka talan vid domstol angående giltigheten av ett beslut om adekvat skyddsnivå

59. Europeiska dataskyddsstyrelsen betonar att även om det i skäl 179 i förslaget till beslut om adekvat skyddsnivå endast hänvisas till situationer där en dataskyddsmyndighet har mottagit ett klagomål som ifrågasätter om ett beslut om adekvat skyddsnivå är förenligt med den enskildes grundläggande rättigheter till integritet och uppgiftsskydd, ska detta uttalande ses som ett exempel på situationer där en dataskyddsmyndighet kan hänskjuta ärendet till en nationell domstol, vilket också skulle vara möjligt utan ett klagomål, snarare än en begränsning av dataskyddsmyndigheternas befogenheter

[21] WP254, s. 3.
[22] WP254, s. 2.
[23] Konvention om skydd för enskilda vid automatisk behandling av personuppgifter, konvention 108+, 18 maj 2018.
[24] Domstolens dom av den 6 oktober 2015 i mål C- 362/14, Maximillian Schrems/Data Protection Commissioner.

enligt GDPR och medlemsstaternas nationella lagstiftning i detta avseende. Bestämmelserna i GDPR omfattar faktiskt både befogenheten att skjuta upp överföringar av uppgifter, även när de grundas på ett beslut om adekvat skyddsnivå, och att väcka talan angående giltigheten av ett beslut om adekvat skyddsnivå, och är inte begränsade till situationer där myndigheterna har mottagit ett klagomål, om deras nationella lagstiftning ger dem befogenhet att göra detta mer allmänt och oberoende av ett klagomål, i enlighet med de relevanta bestämmelserna i GDPR.

60. **Europeiska dataskyddsstyrelsen uppmanar kommissionen att i sitt förslag till beslut om adekvat skyddsnivå klargöra att tillsynsmyndigheternas befogenhet att väcka talan angående giltigheten av ett beslut om adekvat skyddsnivå efter ett klagomål endast är ett exempel på dataskyddsmyndigheternas mer långtgående befogenheter enligt GDPR, vilket omfattar befogenheten att skjuta upp överföringar och att väcka talan angående giltigheten av ett beslut om adekvat skyddsnivå även om det inte föreligger något klagomål, om detta föreskrivs i den nationella lagstiftningen i fråga.**

3 KOMMERSIELLA ASPEKTER

3.1 Innehållsmässiga principer

61. I kapitel 3 i referensramen för adekvat skyddsnivå behandlas innehållsmässig principer. Ett tredjelands eller en internationell organisations system måste innehålla dessa principer för att den skyddsnivå som tillhandahålls ska anses väsentligen likvärdig med den skyddsnivå som garanteras genom EU-lagstiftningen. Europeiska dataskyddsstyrelsen medger att det japanska rättssystemet tillämpar ett annat tillvägagångssätt än det i GDPR för att ge verkan åt rätten till integritet. Rätten till integritet är visserligen inte i sig reglerad i den japanska författningen, men den har erkänts som en konstitutionell rättighet genom rättspraxis, till vilket även hänvisas i kommissionens beslut[25].

62. I synnerhet mot bakgrund av att det japanska tillvägagångssättet tydligt skiljer sig från EU:s tillvägagångssätt krävs det en noggrann granskning, inte bara av enskilda aspekter, utan av hela systemet för att fastställa om det i slutändan tillhandahåller en ”väsentligen likvärdig” skyddsnivå. Detta innebär att eventuella ”brister” avseende en innehållsmässig princip kan kompenseras av andra aspekter som ger tillräckliga kontroller och motvikter.

3.1.1 Begrepp

63. På grundval av referensramen för adekvat skyddsnivå bör grundläggande begrepp och/eller principer rörande skydd av personuppgifter vara definierade i tredjelandets rättsliga ram. Även om dessa begrepp och principer inte exakt behöver återspegla terminologin i GDPR, bör de avspegla och vara i enlighet med de begrepp som används i EU:s dataskyddslagstiftning. Till exempel innehåller GDPR följande viktiga begrepp: ”personuppgifter”, ”behandling av personuppgifter”, ”personuppgiftsansvarig”, ”personuppgiftsbiträde”, ”mottagare” och ”känsliga uppgifter”[26].

64. Personuppgiftslagen innehåller också ett antal definitioner, bland annat ”personlig information”, ”personuppgifter”, ”näringsidkare som hanterar personuppgifter”. **Emellertid verkar**

[25] Europeiska dataskyddsstyrelsen har inte erhållit någon engelsk översättning av detta domstolsbeslut. Se kommissionens genomförandebeslut av den XXXX, i enlighet med Europaparlamentets och rådets förordning (EG) nr 2016/679 om ett adekvat skydd av personuppgifter i Japan, som skickades till Europeiska dataskyddsstyrelsen den 13 november 2018, fotnot 9.
[26] WP254, s. 4.

personuppgiftslagen inte innehålla någon definition av begreppet ”hantering av personuppgifter” som liknar begreppet ”behandling av personuppgifter”.

65. Vad gäller definitionen av begreppet ”hantering av personuppgifter” har PPC tillhandahållit skriftliga svar på Europeiska dataskyddsstyrelsens fråga om denna definition. Kommissionen har citerat detta svar i förslaget till kommissionens beslut ”[i] personuppgiftslagen används inte begreppet ”behandling” utan i stället används det likvärdiga begreppet ”hantering” som, enligt den information som PPC tillhandahållit, omfattar ”varje handling som rör personuppgifter” inklusive förvärv, inmatning, ackumulering, organisering, lagring, redigering/bearbetning, förnyelse, utmatning, säkring, resultat, användning eller tillhandahållande av personlig information.”[27]

66. Eftersom det inte har tillhandahållits några dokument som styrker denna definition uppmanar Europeiska dataskyddsstyrelsen **kommissionen att noga övervaka att definitionen av ovannämnda begrepp, såsom den tillhandahållits av PPC, verkligen följs i praktiken**.

3.1.1.1 Begreppet personuppgiftsbiträde och skyldigheter från en ”förvaltare”

67. Såsom angetts ovan krävs det enligt referensramen för adekvat skyddsnivå att grundläggande begrepp och/eller principer rörande skydd av personuppgifter är definierade i tredjelandets rättsliga ram.

68. Personuppgiftslagen innehåller en definition av ”näringsidkare som hanterar personuppgifter”, vilken enligt kommissionen omfattar både begreppen personuppgiftsansvarig och personuppgiftsbiträde som föreskrivs i GDPR och inte gör någon åtskillnad mellan de två[28]. Personuppgiftslagen innehåller emellertid även begreppet ”förvaltare” i artikel 22, vilket i visst hänseende liknar begreppet personuppgiftsbiträde i GDPR.

69. Såsom PPC har förklarat i de svar som Europeiska dataskyddsstyrelsen har erhållit, och vilka även ingår i kommissionens förslag till beslut om adekvat skyddsnivå, anses en förvaltare vara likvärdig med ett personuppgiftsbiträde enligt GDPR, och har anförtrotts hantering av personuppgifter av en näringsidkare som hanterar personuppgifter. Denna förvaltare har samma skyldigheter och rättigheter som näringsidkaren som hanterar personuppgifter, inklusive de som föreskrivs i tilläggsreglerna för personuppgifter som överförs från EU. Den näringsidkare som hanterar personuppgifter som överlåter hanteringen av personuppgifter till en förvaltare är skyldig att utöva ”nödvändig och lämplig tillsyn”[29] över förvaltaren.

70. **Europeiska dataskyddsstyrelsen uppmanar kommissionen att förklara förvaltarens status och skyldigheter när förvaltaren ändrar ändamålen och medlen för behandlingen och klargöra om den registrerades samtycke fortfarande är en nödvändig förutsättning för ett sådant ändrat syfte eller fastställande av medel[30].**

3.1.1.2 Begreppet lagrade personuppgifter

71. Personuppgiftslagen innehåller begreppet ”lagrade personuppgifter” som anses vara en underkategori av personuppgifter. Enligt personuppgiftslagen är bestämmelserna som rör den registrerades

[27] Kommissionens genomförandebeslut av den XXXX, i enlighet med Europaparlamentets och rådets förordning (EG) nr 2016/679 om ett adekvat skydd av personuppgifter i Japan, som skickades till Europeiska dataskyddsstyrelsen den 13 november 2018, skäl 17.

[28] Kommissionens genomförandebeslut av den XXXX, i enlighet med Europaparlamentets och rådets förordning (EG) nr 2016/679 om ett adekvat skydd av personuppgifter i Japan, som skickades till Europeiska dataskyddsstyrelsen den 13 november 2018, skäl 35.

[29] Artikel 22 i den ändrade lagen om skydd av personuppgifter (personuppgiftslagen), som trädde i kraft den 30 maj 2017.

[30] Artikel 23.5 i) i personuppgiftslagen. Se även avsnittet om öppenhetsprincipen nedan.

rättigheter[31] endast tillämpliga på lagrade personuppgifter. Definitionen av lagrade personuppgifter ingår i artikel 2.7 i personuppgiftslagen.

72. Lagrade personuppgifter är personuppgifter som inte ska i) raderas inom en period på högst sex månader[32] eller som ii) omfattas av undantagen i artikel 4 i regeringsdekretet, och som sannolikt kan skada allmänna intressen eller andra intressen, om deras förekomst eller frånvaro blir känd.

73. I tilläggsregel 2 föreskrivs att ”personuppgifter som erhålls från EU på grundval av ett beslut om adekvat skyddsnivå ska hanteras som lagrade personuppgifter oberoende av inom vilken period uppgifterna ska raderas”.

74. Personuppgifter som omfattas av undantagen i artikel 4 i regeringsdekretet behöver dock inte behandlas som lagrade personuppgifter, och registrerades rättigheter är inte tillämpliga.

75. I artikel 23 i GDPR anges, i likhet med i artikel 4 i regeringsdekretet, att unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige/personuppgiftsbiträdet omfattas av, kan begränsa omfattningen av de skyldigheter som är tillämpliga på denne och de rättigheter som är tillgängliga för den registrerade. Detta kan göras genom en lagstiftningsåtgärd. Sådana begränsningar måste respektera andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle.

76. Vad gäller innehållet i de undantag som föreskrivs i artikel 4 i regeringsdekretet har Europeiska dataskyddsstyrelsen inte erhållit tillräcklig dokumentation om dessa begränsningar eller ytterligare aspekter för att klargöra tillämpningsområdet för dessa bestämmelser.[33] Europeiska dataskyddsstyrelsen kan inte bedöma om dessa begränsningar av de registrerades rättigheter är begränsade till vad som kan anses vara strikt nödvändigt och proportionerligt enligt unionslagstiftningen, och därför skulle vara väsentligen likvärdiga med de rättigheter som de registrerade i EU har.

77. **På grund av avsaknaden av vissa relevanta dokument välkomnar Europeiska dataskyddsstyrelsen även försäkringar från kommissionen, om begränsningar av enskilda personers rättigheter (i synnerhet rätten till tillgång, rättelse och invändningar) är nödvändiga och proportionerliga i ett demokratiskt samhälle och respekterar grundprinciperna som ligger till grund för de grundläggande rättigheterna.**

78. Ett väsentligt krav enligt GDPR är att personuppgifter skyddas under hela deras livscykel.

79. Med hänsyn till att tilläggsreglerna endast är tillämpliga på personuppgifter som överförs från EU skulle Europeiska dataskyddsstyrelsen uppskatta att få ytterligare information om den praktiska tillämpningen av dessa regler från näringsidkare som hanterar personuppgifter, särskilt när dessa uppgifter vidarebefordras till en annan näringsidkare som hanterar personuppgifter efter att de har överförts till Japan första gången.

80. Kommissionen har i skäl 15 i sitt förslag till beslut om adekvat skyddsnivå klargjort att näringsidkare som hanterar personuppgifter som tar emot och/eller ytterligare behandlar personuppgifter från EU,

[31] Artiklarna 27–30 i personuppgiftslagen.

[32] Ändring av regeringsdekretet för att genomföra lagen om skydd av personuppgifter (regeringsdekretet), som trädde i kraft den 30 maj 2017, artikel 5.

[33] Europeiska dataskyddsstyrelsen har inte erhållit det beslut från högsta domstolen som det hänvisas till i skäl 53 i förslaget till beslut om adekvat skyddsnivå.

kommer att ha en rättslig skyldighet att följa tilläggsreglerna och att de för att kunna göra detta måste säkerställa att de kan identifiera sådana personuppgifter under hela deras livscykel.

81. I sina svar förklarade PPC[34] att denna identifiering kommer att göras med hjälp av tekniska metoder (märkning) eller organisatoriska metoder (lagring av uppgifter från EU i en särskild databas).

82. I fotnot 14 i sitt förslag till beslut om adekvat skyddsnivå förklarar kommissionen att näringsidkare som hanterar personuppgifter måste registrera informationen om EU-uppgifternas ursprung så länge som det är nödvändigt för att de ska kunna följa tilläggsreglerna. Detta fastställs också i artikel 26.1 och 26.3–4 i personuppgiftslagen, där det anges att en näringsidkare som hanterar personuppgifter är skyldig att bekräfta och registrera källan till dessa uppgifter och alla omständigheter som har samband med förvärvet av dessa uppgifter.

83. Europeiska dataskyddsstyrelsen noterar dock att det i artikel 18 i genomförandebestämmelserna till personuppgiftslagen[35] anges att registreringsskyldigheten för näringsidkare som hanterar personuppgifter är begränsad till högst tre år när det gäller situationer som inte omfattas av de särskilda registreringsmetoder som beskrivs i artikel 16 i genomförandebestämmelserna (användning av ett skriftligt dokument, elektromagnetisk registrering eller mikrofilm). Detta påpekas även av kommissionen i skäl 71 i förslaget till beslut om adekvat skyddsnivå: ”Såsom anges i artikel 18 i genomförandebestämmelserna ska dessa register bevaras i ett till tre år, beroende på omständigheterna”.

84. Även om det, såsom kommissionen har uppgett i fotnot 14 i sitt förslag till beslut om adekvat skyddsnivå, inte är förbjudet för näringsidkare som hanterar personuppgifter att föra register över uppgifternas ursprung i över tre år för att de ska kunna fullgöra sina skyldigheter enligt tilläggsregel 2, framgår inte detta tydligt av den japanska lagstiftningen eller av tilläggsreglerna. Europeiska dataskyddsstyrelsen anser att det finns en risk att näringsidkare som hanterar personuppgifter i praktiken kommer att följa artikel 18 i genomförandebestämmelserna även när de behandlar uppgifter från EU. Detta beror främst på att det för närvarande, såsom Europeiska dataskyddsstyrelsen har förstått och på grundval av tillgängliga dokument, inte finns någon bestämmelse som ålägger näringsidkare som hanterar personuppgifter en sådan skyldighet att i stället följa tilläggsreglerna. Detta skulle leda till att uppgifter som överförs från EU inte längre skyddas genom det extra skydd som ingår i tilläggsreglerna.

85. **Europeiska dataskyddsstyrelsen uppmanar kommissionen att noga övervaka det effektiva skyddet av personuppgifter som överförs från EU till Japan på grundval av förslaget till beslut om adekvat skyddsnivå under hela deras livscykel, även om den japanska lagstiftningen föreskriver en registreringsskyldighet avseende uppgifternas ursprung under högst tre år.**

3.1.2 Grunder för laglig och rättvis behandling för berättigade ändamål

86. Enligt referensramen för adekvat skyddsnivå måste uppgifterna, i enlighet med GDPR, behandlas på ett lagligt, rättvist och berättigat sätt[36]. Den rättsliga grund enligt vilken personuppgifter kan behandlas på ett lagligt, rättvist och berättigat sätt ska anges på ett tillräckligt tydligt sätt. Det finns åtskilliga sådana legitima grunder inom EU:s rättsliga ramar, till exempel bestämmelser i nationell lagstiftning, den registrerades samtycke, fullgörande av ett avtal eller berättigat intresse från den personuppgiftsansvariges eller en tredje parts sida när inte individens intressen väger tyngre.

[34] Bilaga III till detta yttrande.

[35] Genomförandebestämmelser till lagen om skydd av personuppgifter (nedan kallade *genomförandebestämmelserna*), som trädde i kraft den 30 maj 2017, artikel 16.

[36] WP254, s. 4.

87. Enligt personuppgiftslagen spelar samtycke en central roll i det japanska rättsliga systemet för uppgiftsskydd. Samtycke utgör den centrala rättsliga grunden för behandling av personuppgifter i Japan och är även en av de huvudsakliga rättsliga grunderna för överföring av personuppgifter från Japan till ett tredjeland. Dessutom krävs samtycke för en ändring av syftet med behandlingen.

88. Enligt tilläggsregel 3 ska den rättsliga grunden för behandling av personuppgifter som överförs från EU till Japan vara den rättsliga grund för vilken uppgifterna överförts till Japan. Om en näringsidkare som hanterar personuppgifter vill behandla dessa uppgifter ytterligare för ett annat ändamål måste denne på förhand inhämta den registrerades samtycke.

89. Europeiska dataskyddsstyrelsen anser att kvaliteten på samtycket, särskilt på grund av dess centrala roll i den japanska rättsliga ramen, måste uppfylla de grundläggande krav som ställs på begreppet samtycke, dvs. enligt EU-lagstiftningen, en ”frivillig, specifik, informerad och otvetydig viljeyttring...” från den registrerade. Den registrerade kan återkalla ett sådant samtycke som ett viktigt skydd för att säkerställa den registrerades fria vilja under hela tiden[37]. Rätten att återkalla samtycket, som en obligatorisk del av samtycket, förefaller saknas i den japanska rättsliga ramen. Enligt genomförandebestämmelserna[38] är ett återkallande av samtycket endast ”önskvärt” och är beroende av ”affärsverksamhetens egenskaper, storlek och status”.

3.1.3 Öppenhetsprincipen

90. På grundval av artikel 5 GDPR är öppenhet en grundläggande princip i EU:s system för uppgiftsskydd.[39] I referensramen för adekvat skyddsnivå anges ”öppenhet” uttryckligen som en av de innehållsmässiga principer som ska beaktas vid bedömningen av den väsentligen likvärdiga skyddsnivå som tillhandahålls av ett tredjeland. Principen om öppenhet och rättvisa har i syfte att säkerställa att den registrerade har kontroll över sina uppgifter och mot denna bakgrund ska den registrerade i regel erhålla information på ett proaktivt sätt. När det gäller skölden för skydd av privatlivet hänvisade artikel 29-arbetsgruppen[40] i sitt yttrande 1/2016 till bilaga II, II 1 b till avtalet om skölden för skydd av privatlivet (meddelande till den enskilde) och uppgav att om uppgifterna inte samlas in direkt bör en organisation informera den registrerade ”vid det tillfälle då uppgifterna registreras av den organisation som är ansluten till skölden för skydd av privatlivet” (avsnitt 2.2.1 a). Ett ytterligare kriterium är att det föreligger offentlig tillgång till integritetsskyddspolicyn (se avsnitt 2.2.1 b). Således ansågs det redan nödvändigt att direkt informera den registrerade enligt direktiv 95/46/EG.

91. En första farhåga uppkommer rörande det sätt på vilket informationen tillhandahålls den registrerade enligt personuppgiftslagen. Enligt artikel 27.1 i personuppgiftslagen är en näringsidkare som hanterar personuppgifter skyldig att lämna den information som anges i artikel 27.1 i personuppgiftslagen genom att se till att den ”är i ett sådant skick att huvudmannen kan ha kännedom”. Denna formulering

[37] Artikel 4.11 GDPR. För ytterligare information, se även Europeiska dataskyddsstyrelsens relevanta riktlinjer om samtycke, WP259, av den 10 april 2018.

[38] Data Protection Legal and Technical Research and Analysis Consortium (DPC), An assessment of the level of protection of personal data provided under Japanese law, s. 46: ”Med hänsyn till skyddet för rättigheter och intressen från en huvudman såsom en konsument är det önskvärt, om man har fått en begäran från en huvudman som rör de lagrade personuppgifterna, att ytterligare reagera på huvudmannens efterfrågan på ett sådant sätt som att upphöra med att skicka direkt post eller att frivilligt upphöra med utnyttjandet osv. med beaktande av affärsverksamhetens egenskaper, storlek och status.”

[39] WP 254, kapitel 3, punkt 7, s. 5, se även skäl 39 GDPR.

[40] Denna arbetsgrupp inrättades enligt artikel 29 i direktiv 95/46/EG. Den var ett oberoende rådgivande EU-organ i frågor om integritet och dataskydd. Dess uppgifter beskrivs i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG. Artikel 29-gruppen har nu blivit Europeiska dataskyddsstyrelsen.

klargör dock inte i vilken utsträckning en näringsidkare som hanterar personuppgifter är skyldig att vidta positiva åtgärder för att verkligen informera den registrerade.

92. **Europeiska dataskyddsstyrelsen uppmanar kommissionen att klargöra innebörden av begreppet ”kan ha kännedom” och huruvida det i regel föreskrivs en skyldighet i personuppgiftslagen att verkligen informera de registrerade.**

93. Dessutom kan det, i enlighet med referensramen för adekvat skyddsnivå, föreligga begränsningar av den information som ska lämnas till den registrerade, liknande de i artikel 23 GDPR. På liknande sätt föreskrivs ett undantag från rätten till information när uppgifterna sannolikt kommer att göra det omöjligt eller avsevärt försvårar uppfyllandet av behandlingen i artikel 14.5 GDPR. Även i detta fall ska den personuppgiftsansvarige emellertid tillhandahålla någon form av information, t.ex. genom att göra ”generaliserad” information tillgänglig för allmänheten. Dessutom ska den registrerade informeras när risken upphör[41]. Dessa aspekter är viktiga för att säkerställa den grundläggande principen om rättvisa.

94. Enligt artikel 23 i personuppgiftslagen har en näringsidkare som hanterar personuppgifter en allmän skyldighet att informera den registrerade i förväg om dennes uppgifter tillhandahålls en tredje part antingen underförstått när samtycket erhålls eller uttryckligen genom ett meddelande om undantag. Europeiska dataskyddsstyrelsen uppfattar det som att den registrerade inte erhåller något meddelande som informerar vederbörande om att hans eller hennes uppgifter inte utgör lagrade personuppgifter enligt personuppgiftslagen, eftersom de omfattas av undantagen i artikel 4 i regeringsdekretet. Mot denna bakgrund kan de inte dra full nytta av sina rättigheter. De registrerade informeras inte heller i de situationer som anges i artikel 18.4 i personuppgiftslagen.

95. **Europeiska dataskyddsstyrelsen konstaterar att rättigheterna kan begränsas på grund av legitima mål från den näringsidkare som hanterar personuppgifter och de statliga myndigheterna. Samtidigt anser Europeiska dataskyddsstyrelsen att det i förväg åtminstone bör lämnas allmän information om möjligheten att begränsa rättigheterna mot bakgrund av de mål som avses i lagen och att den registrerade bör meddelas när de risker på grund av vilka informationen begränsas upphör.**

96. Slutligen behandlas andra aspekter av öppenhet och insyn ytterligare nedan. Dessa hänför sig till de risker som överföringen till ett tredjeland medför[42] och information om syfte med behandling i samband med automatiserat beslutsfattande, inbegripet profilering.[43]

3.1.4 Begränsningar för vidare överföring

97. Europeiska dataskyddsstyrelsen välkomnar ansträngningarna från de japanska myndigheterna och kommissionen att förbättra skyddsnivån för vidare överföringar i tilläggsregel 4, vilken utesluter att personuppgifter som överförts från EU överförs vidare till ett tredjeland på grundval av APEC:s CBPR-bestämmelser. Dessutom erkänner Europeiska dataskyddsstyrelsen att kommissionen i skälen 177–184 i sitt nya förslag till beslut om adekvat skyddsnivå har åtagit sig att upphäva beslutet om adekvat skyddsnivå när ett fortsatt skydd inte längre är säkerställt vid vidare överföringar. Europeiska dataskyddsstyrelsen skulle dock vilja behandla två aspekter när det gäller dessa överföringar från Japan av personuppgifter från EU till tredjeländer.

98. **Användningen av samtycke som grund för överföring av uppgifter från Japan till ett tredjeland i det japanska rättssystemet ger upphov till farhågor, eftersom Europeiska dataskyddsstyrelsen anser att**

[41] Domstolens dom av den 21 december 2016 i de förenade målen C-203/15 och C-698/15, Tele2, skäl 121 och domstolens dom av den 8 april 2014 i de förenade målen C-293/12 och C-594/12, Digital Rights Ireland, skäl 54–62.
[42] Se avsnitt 2.1.4.
[43] Se avsnitt 2.1.6.

den information som lämnas till registrerade i EU innan samtycke lämnas inte förefaller vara heltäckande.

99. Enligt artikel 24 i personuppgiftslagen är det förbjudet att överföra personuppgifter till en tredje part utanför Japans territorium utan att först ha inhämtat den berörda personens samtycke. I tilläggsregel 4 föreskrivs att registrerade i EU ska erhålla den information om omständigheterna kring överföringen som krävs för att fatta ett beslut om deras samtycke.

100. Kommissionen bedömer i sitt förslag till beslut om adekvat skyddsnivå att tilläggsregel 4 garanterar ett särskilt väl underbyggt samtycke från registrerade i EU,[44] eftersom de kommer att informeras om att uppgifterna kommer att överföras till utlandet och om det specifika destinationslandet. Detta gör det möjligt för den registrerade att bedöma risken för integriteten i samband med överföringen.

101. Enligt öppenhetsprincipen i referensramen för adekvat skyddsnivå ska en viss grad av rättvisa garanteras när enskilda personer informeras. I samband med vidare överföringar som grundas på samtycke anser Europeiska dataskyddsstyrelsen att de registrerade, för att säkerställa en sådan adekvat nivå av rättvisa, uttryckligen bör informeras om de möjliga riskerna med sådana överföringar som uppkommer för att det saknas ett tillräckligt skydd i tredjelandet och att det saknas lämpliga skyddsåtgärder innan de lämnar sitt samtycke. Ett sådant meddelande bör t.ex. innehålla information om att det kanske saknas tillsynsmyndighet i tredjelandet och/eller att principer för behandling av uppgifter och/eller den registrerades rättigheter kanske inte tillhandahålls i tredjelandet[45]. För Europeiska dataskyddsstyrelsen är tillhandahållandet av denna information av avgörande betydelse för att den registrerade ska kunna ge sitt samtycke med full kännedom om dessa specifika omständigheter för överföringen[46].

102. Informerat samtycke är också viktigt när det gäller sektorsspecifika undantag. Beslutet om adekvat skyddsnivå omfattar inte vissa typer av behandling som utförs av vissa organ, såsom universitet, vid behandling av personuppgifter för akademiska ändamål. Europeiska dataskyddsstyrelsens farhågor i detta avseende hänför sig till det särskilda scenariot när uppgifter som överförs från EU i enlighet med beslutet om adekvat skyddsnivå – till exempel personuppgifter från Erasmusstudenter i Japan – sedan används för ett annat ändamål som inte omfattas av tillämpningsområdet för beslutet om adekvat skyddsnivå (t.ex. forskningsändamål), med samtycke från den registrerade, och omfattas därför inte längre av det ytterligare skydd som tillhandahålls genom tilläggsreglerna.

103. Kommissionen anger i skäl 38 i sitt förslag till beslut om adekvat skyddsnivå att ett sådant scenario kommer att omfattas av ramen för vidare överföringar och att en näringsidkare som hanterar personuppgifter i sådana fall måste förse den registrerade med all nödvändig information innan denne ger sitt samtycke, inbegripet att personuppgifterna inte omfattas av skyddet enligt bestämmelserna i personuppgiftslagen.

104. Enligt tilläggsregel 4 krävs endast att näringsidkaren som hanterar personuppgifter erhåller samtycke från den registrerade efter att ha erhållit information om omständigheterna kring den överföring som krävs för att huvudmannen ska kunna fatta ett beslut om sitt samtycke.

---

[44] Kommissionens genomförandebeslut av den XXXX, i enlighet med Europaparlamentets och rådets förordning (EG) nr 2016/679 om ett adekvat skydd av personuppgifter i Japan, som skickades till Europeiska dataskyddsstyrelsen den 13 november, skäl 76.

[45] Europeiska dataskyddsstyrelsens riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679, 25 maj 2018, s. 8.

[46] Europeiska dataskyddsstyrelsens riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679, 25 maj 2018, s. 7.

105. **Europeiska dataskyddsstyrelsen uppmanar kommissionen att se till att den information som ska lämnas till den registrerade ”om omständigheterna kring överföringen” omfattar information om de möjliga riskerna från överföringar till följd av att det saknas ett tillräckligt skydd i tredjelandet och avsaknaden av lämpliga skyddsåtgärder, eller i fråga om sektorsspecifika undantag, om avsaknaden av skydd enligt tilläggsreglerna och personuppgiftslagen.**

106. **Vidare överföring av personuppgifter kan ske till tredjeländer som kan bli föremål för ett senare japanskt beslut om adekvat skyddsnivå.**

107. Utan att det påverkar tillämpningen av de undantag som föreskrivs i artikel 23.1 i personuppgiftslagen, kan uppgifter som ursprungligen har överförts från EU till Japan sedan överföras från Japan till ett tredjeland utan samtycke i två situationer:

- Om näringsidkaren som hanterar personuppgifter och den mottagande tredje parten tillsammans har genomfört åtgärder för att tillhandahålla en skyddsnivå som är likvärdig med den i personuppgiftslagen jämförd med tilläggsreglerna genom ett avtal, andra former av bindande överenskommelser eller bindande överenskommelser inom en koncern[47].

- Om PPC enligt artikel 24 i personuppgiftslagen och artikel 11 i genomförandebestämmelserna[48] har erkänt att tredjelandet tillhandahåller en skyddsnivå som är likvärdig med det som garanteras i Japan.

108. Europeiska dataskyddsstyrelsen anser att artikel 24 i personuppgiftslagen utgör den mer specifika bestämmelsen som innehåller ett undantag från den allmänna regeln i artikel 23 i personuppgiftslagen. Därför instämmer Europeiska dataskyddsstyrelsen inte i kommissionens bedömning i den nya sista meningen i skäl 78 i förslaget till beslut om adekvat skyddsnivå, där det anges att överföringen till den tredje parten även i dessa situationer fortfarande omfattas av kravet på att erhålla samtycke enligt artikel 23.1 i personuppgiftslagen.

109. Enligt artikel 11.1 i genomförandebestämmelserna kräver ett beslut om adekvat skyddsnivå från PPC materiella standarder som är likvärdiga med de i personuppgiftslagen, vars genomförande är säkerställda i tredjelandet och som övervakas effektivt av en oberoende tillsynsmyndighet. Dessutom kan PPC införa nödvändiga villkor för att skydda rättigheter och intressen från enskilda i Japan, i enlighet med artikel 11.2 i genomförandebestämmelserna.

110. Enligt tilläggsregel 4 kan personuppgifter från EU utan ytterligare begränsningar överföras till ett tredjeland som omfattas av ett japanskt beslut om adekvat skyddsnivå. Enligt artikel 44 GDPR föreskrivs emellertid att all överföring av personuppgifter till ett tredjeland måste uppfylla villkoren i kapitel V i GDPR, inbegripet vidare överföring från tredjelandet till ett annat tredjeland. Skyddsnivån för de fysiska personer vars personuppgifter överförs får inte undergrävas av den vidare överföringen[49]. Även om kommissionen i princip även instämmer i denna tolkning i dess förslag till beslut om adekvat skyddsnivå[50], förefaller den inte följas fullständigt. Kommissionen har förhandlat fram ett förbud mot överföring av uppgifter från EU till ett tredjeland på grundval av APEC:s CBPR-

[47] Tilläggsregel 4 ii.

[48] Genomförandebestämmelser för lagen om skydd av personuppgifter av den 30 maj 2017. Europeiska dataskyddsstyrelsen har erhållit en engelsk översättning av den nya artikel 11 från kommissionen, men denna artikel har ännu inte offentliggjorts.

[49] WP 254, s. 5.

[50] Kommissionens genomförandebeslut av den XXXX, i enlighet med Europaparlamentets och rådets förordning (EG) nr 2016/679 om ett adekvat skydd av personuppgifter i Japan, som skickades till Europeiska dataskyddsstyrelsen den 13 november, skäl 75.

bestämmelser. Mot bakgrund av det jämförande verktyg som utvecklats under 2014 inom ramen för EU-direktivet mellan bindande företagsregler (Binding Corporate Rules, BCR) och CBPR som visar kraven från båda systemen, deras likheter och skillnader (artikel 29-arbetsgruppens yttrande 02/2014), hyser Europeiska dataskyddsstyrelsen farhågor när det gäller användningen av CBPR-bestämmelser som verktyg för vidare överföring av personuppgifter som överförs från EU till länder utanför Japan.

111. Däremot förefaller kommissionen godta vidare överföringar av personuppgifter som överförts från EU till Japan på grundval av ett japanskt beslut om adekvat skyddsnivå, utan att PPC har möjlighet att föreskriva att tilläggsreglerna ska tillämpas för att skydda rättigheter och intressen från enskilda personer i EU, i förekommande fall. Av artikel 44 GDPR sluter sig Europeiska dataskyddsstyrelsen till att det förbättrade skydd för uppgifter som överförs från EU till Japan som föreskrivs i tilläggsreglerna alltid måste utvidgas när personuppgifter som överförs från EU till Japan överförs vidare till ett tredjeland, om ramverket för uppgiftsskydd i det landet inte har erkänts som väsentligen likvärdigt med GDPR.

112. **Europeiska dataskyddsstyrelsen uppmanar därför kommissionen att ta över sin övervakande roll och se till att skyddsnivån för uppgifter från EU bibehålls eller att överväga att upphäva detta beslut om adekvat skyddsnivå om personuppgifter som överförts från EU till Japan överförs vidare till tredjeländer som omfattas av ett eventuellt senare japanskt beslut om adekvat skyddsnivå, när dessa tredjeländer inte har varit föremål för en tidigare bedömning eller ett beslut om adekvat skyddsnivå i EU.**

3.1.5 Direkt marknadsföring

113. Enligt tilläggsregel 3 får en näringsidkaren som hanterar personuppgifter inte behandla uppgifter för direktmarknadsföring om de har överförts från Europeiska unionen för ett annat ändamål och den registrerade i EU inte har samtyckt till att användningssyftet ändras.

114. Enligt referensramen för adekvat skyddsnivå ska den registrerade om personuppgifter behandlas för direktmarknadsföring ha möjlighet att när som helst och utan kostnad invända mot att dennes uppgifter behandlas för detta syfte. Enligt artikel 16 i personuppgiftslagen får en näringsidkare som hanterar personuppgifter endast behandla personuppgifter om den registrerade ger sitt samtycke. Återkallandet av samtycket skulle kunna ge samma resultat som den priviligierade rätten att invända mot direktmarknadsföring.

115. Den japanska ramen för uppgiftsskydd ger inte någon privilegierad invändningsrätt och såsom förklaras ovan i avsnittet om samtycke är ett återkallande av samtycke enligt genomförandebestämmelserna endast önskvärt och villkorat och kan därför inte anses vara likvärdig med en rätt att när som helst göra invändningar såsom krävs enligt referensramen för adekvat skyddsnivå. **Europeiska dataskyddsstyrelsen uppmanar kommissionen att tillhandahålla försäkringar om rätten att återkalla samtycke och att övervaka ärenden som rör direktmarknadsföring.**

3.1.6 Automatiserat beslutsfattande och profilering

116. Enligt referensramen för adekvat skyddsnivå kan beslut som enbart baseras på automatisk behandling (automatiserat individuellt beslutsfattande), inklusive profilering, som får rättsliga följder för eller i betydande grad påverkar den registrerade, endast äga rum under vissa villkor som fastställs i tredjelandets rättsliga ramar. Under de ovannämnda omständigheterna krävs därför en rättslig grund varje gång ett automatiskt beslutsfattande och en profilering äger rum.

117. Inom EU:s ramverk omfattar villkoren för automatiserat beslutsfattande t.ex. behovet av att inhämta ett uttryckligt samtycke[51] från den registrerade eller att det krävs ett sådant beslut för att ett avtal ska kunna ingås. Om beslutet inte uppfyller sådana villkor som fastställs i tredjelandets rättsliga ram bör den registrerade ha rätt att inte omfattas av det. Dessutom bör det i tredjelandets lagstiftning under alla omständigheter föreskrivas nödvändiga skyddsåtgärder, inbegripet rätten att få information om de särskilda skäl som ligger till grund för beslutet och det logiska systemet för att korrigera felaktiga eller ofullständiga uppgifter och bestrida beslutet om det har antagits på felaktiga grunder.

118. I kommissionens beslut hänvisas endast till banksektorn, där sektorsspecifika bestämmelser[52] om automatiserade beslut är tillämpliga. De övergripande riktlinjerna för tillsyn över stora banker som anges i skäl 93 i förslaget till beslut om adekvat skyddsnivå talar för att den berörda personen måste erhålla särskilda förklaringar varför en ansökan om att ingå ett låneavtal har avslagits.

119. De argument som kommissionen hänvisar till i förslaget till beslut om adekvat skyddsnivå (skäl 94), att avsaknaden av särskilda regler för automatiserat beslutsfattande i personuppgiftslagen sannolikt inte kommer att påverka skyddsnivån, förefaller (till exempel) inte beakta situationer när personuppgifter som överförts från EU senare behandlas av en annan japansk personuppgiftsansvarig (en annan än den ursprungliga japanska importören av uppgifter).

120. Det förefaller därför inte finnas några allmänna regler som är tillämpliga mellan olika sektorer i Japan när det gäller automatiserat beslutsfattande och profilering.

121. **Europeiska dataskyddsstyrelsen uppmanar kommissionen att övervaka ärenden som rör automatiserat beslutsfattande och profilering.**

3.2 Förfarande- och verkställandemekanismer

122. Med utgångspunkt i de kriterier som anges i referensramen för adekvat skyddsnivå har Europeiska dataskyddsstyrelsen analyserat följande aspekter av den japanska rättslig ramen och ramen för uppgiftsskydd som omfattas av förslaget till beslut om adekvat skyddsnivå: huruvida det finns eller inte finns en oberoende tillsynsmyndighet som fungerar effektivt, ett system som säkerställer en god nivå av överensstämmelse och ett system med tillgång till lämpliga prövningsmekanismer som ger enskilda personer i EU möjlighet att utöva sina rättigheter och begära prövning utan att mötas av omständliga hinder för administrativ och rättslig prövning.

123. På grundval av de kriterier som EU-domstolen har fastställt i domen i målet Schrems[53] och de kriterier som anges i skäl 104 och i artikel 45 GDPR anser Europeiska dataskyddsstyrelsen att även om det föreligger ett system i Japan som är förenligt med EU:s kan det vara svårt i praktiken att få tillgång till detta system för enskilda personer i EU, vars uppgifter kommer att överföras enligt detta beslut om adekvat skyddsnivå mot bakgrund av förekomsten av språkliga och institutionella hinder.

124. I nedanstående avsnitt ska de ovannämnda aspekterna av den japanska ramen granskas innan några rekommendationer för kommissionen lyfts fram.

3.2.1 Oberoende behörig tillsynsmyndighet

125. PPC inrättades den 1 januari 2016 efter ändringarna av personuppgiftslagen år 2015 och ersatte sin föregångare – den särskilda kommissionen för skydd av personuppgifter (vilken inrättades 2013 enligt My Number Act). Även om det är frågan om en ung organisation har PPC sedan inrättandet gjort stora

[51] För kritik mot begreppet samtycke i den japanska rättsliga ramen för uppgiftsskydd, se 2.1. Allmänt och 2.2.8. Direkt marknadsföring.

[52] Europeiska dataskyddsstyrelsen har inte erhållit dessa sektorsspecifika bestämmelser.

[53] Mål C-362/14 (2015) Maximilian Schrems/Data Protection Commissioner (punkterna 73 och 74).

ansträngningar för att bygga upp den infrastruktur som krävs för att kunna genomföra den ändrade personuppgiftslagen. Bland dessa märks bland annat fastställandet av genomförandebestämmelserna, PPC:s riktlinjer för att ge vägledning till näringsidkare som hanterar personuppgifter, offentliggörandet av ett dokument med frågor och svar från PPC[54] och inrättandet av en telefonlinje för att ge företag och privatpersoner råd avseende bestämmelserna om uppgiftsskydd samt av en medlingstjänst för att hantera klagomål.

126. Inrättandet av PPC och myndighetens funktion regleras i kapitel V i personuppgiftslagen. Även om PPC omfattas av premiärministerns behörighet föreskrivs det i artikel 62 att PPC ska utöva sin verksamhet självständigt. Europeiska dataskyddsstyrelsen välkomnar kommissionens klargörande i det ändrade förslaget till beslut om adekvat skyddsnivå som skickades ut den 13 november 2018 för att ytterligare beskriva i vilken omfattning PPC är fritt från internt och externt inflytande.

3.2.2 Systemet för skydd av personuppgifter måste säkerställa en god efterlevnad

127. I förslaget till beslut om adekvat skyddsnivå görs en omfattande granskning av PPC:s befogenheter enligt artiklarna 40, 41 och 42 i personuppgiftslagen för att säkerställa övervakning och genomförande av lagstiftningen. Artikel 40 ger PPC befogenhet att begära att näringsidkare som hanterar personuppgifter inger rapporter och dokumentation om behandlingsverksamheten samt utför inspektioner på plats. Enligt artikel 42 har PPC befogenhet att – när myndigheten fastställer att det är nödvändigt att skydda individuella rättigheter eller vid en överträdelse av lagbestämmelserna – utfärda rekommendationer och, om detta inte ger resultat, föreläggande till näringsidkare som hanterar personuppgifter att upphöra med överträdelsen eller vidta de åtgärder som krävs för att rätta till överträdelsen.

128. I oktober 2018 vidtog PPC en av sina första åtgärder enligt artikel 41 i den ändrade personuppgiftslagen och gav ”anvisningar” till en näringsidkare som hanterar personuppgifter, uppmanade företaget att stärka sina säkerhetsåtgärder och på ett effektivt sätt övervaka tillhandahållare av applikationer och ge användarna tydlig och lättbegriplig information om hur deras personuppgifter används och inhämta samtycke i förväg när informationen delas med en tredje part samt reagera på rätt sätt på användarnas begäran om radering av deras information. I de svar som lämnats till Europeiska dataskyddsstyrelsen[55] uppgav tjänstemän vid PPC att företaget hade meddelat att det kommer att samarbeta och att myndigheten, om företaget underlåter att göra det, kommer att utfärda en ”rekommendation” till företaget enligt artikel 42.1 i personuppgiftslagen.

129. Den undersökning som PPC har genomfört avseende ovannämnda näringsidkare som hanterar personuppgifter är en mycket positiv indikator på den japanska tillsynsmyndighetens ansträngningar att säkerställa en god efterlevnad i landet.

130. Även om det har gjorts förbättringar i det ramverk som gällde före 2015 års ändringar konstaterar Europeiska dataskyddsstyrelsen att PPC har färre befogenheter än den europeiska dataskyddsmyndigheten har enligt GDPR, särskilt när det gäller **kontroll av efterlevnaden**. Till exempel är de administrativa sanktionsavgifterna[56] relativt lindriga. I skäl 108 i kommissionens beslut betonas

[54] Europeiska dataskyddsstyrelsen har inte erhållit detta dokument från kommissionen på engelska.

[55] Bilaga III.

[56] Dessa fastställs i kapitel VII i personuppgiftslagen. De maximala bötesbeloppet föreskrivs i artikel 83 (insamling eller användning genom stöld av en databas med personuppgifter i olagligt vinstsyfte för egen eller en tredje parts räkning) och motsvarar antingen ett års fängelse med straffarbete eller böter på högst 500 000 yen (ungefär 3 900 euro). Enligt de förklaringar som kommissionen har tillhandahållit är böter kumulativa per överträdelse. Även om detta kan vara fallet konstaterar Europeiska dataskyddsstyrelsen att det totala beloppet sannolikt förblir mycket lågt jämfört med EU:s standarder även om ackumulerade böter tillämpas.

att det i fall av bristande efterlevnad eller vissa överträdelser av personuppgiftslagen föreligger straffrättsliga påföljder och att PPC:s ordförande kan vidarebefordra ärenden till åklagarmyndigheten. I kommissionens beslut beaktas emellertid inte att ett allmänt åtal i Japan grundas på en skönsmässig bedömning och ibland kan vara föremål för långdragna översynsförfaranden[57]. Dessutom kan ett fängelsestraff (med eller utan straffarbete) i samband med överträdelser av personuppgiftslagen enligt bestämmelserna i kapitel VII vara svårt att verkställa på grund av att det är riktat till fysiska personer och i vart fall inte straffar en näringsidkare som hanterar personuppgifter i egenskap av juridisk person när denne inte fullgör sin ansvarsskyldighet.

131. **Mot denna bakgrund uppmanar Europeiska dataskyddsstyrelsen kommissionen att noga övervaka effektiviteten från sanktioner och relevanta rättsmedel i det japanska systemet för uppgiftsskydd.**

3.2.3 Systemet för skydd av personuppgifter måste ge stöd och hjälp till enskilda registrerade i deras utövande av sina rättigheter samt tillhandahålla lämpliga prövningsmekanismer

132. PPC tillhandahåller omfattande information och riktlinjer på sin webbplats i syfte att öka medvetenheten bland näringsidkare som hanterar personuppgifter vad gäller deras skyldigheter och ansvar enligt ramen för uppgiftsskydd samt en telefonlinje för att tillhandahålla information och stöd till japanska medborgare när det gäller deras individuella rättigheter enligt personuppgiftslagen. Webbplatsen har också ett avsnitt, ”Children’s room”, som uttryckligen riktar sig till barn och ungdomar. Europeiska dataskyddsstyrelsen noterar att denna information – tillsammans med stöd från telefonlinjen, vägledning och dokumentation om frågor och svar – finns att tillgå på japanska[58]. Därför är Europeiska dataskyddsstyrelsen fast övertygad om att det skulle vara fördelaktigt om PPC kunde tillhandahålla en särskild sida på den engelska versionen av sin webbplats till enskilda personer i EU vars uppgifter kommer att överföras till Japan enligt kommissionens beslut om adekvat skyddsnivå i syfte att tillhandahålla information om deras individuella rättigheter enligt den japanska ramen för uppgiftsskydd och enligt tilläggsreglerna.

133. Europeiska dataskyddsstyrelsen välkomnar kommissionens förtydligande i skäl 104 i det ändrade förslaget till beslut om adekvat skyddsnivå som skickades ut den 13 november 2018 beträffande den medlingstjänst som PPC tillhandahåller i enlighet med artikel 61 ii i personuppgiftslagen. Europeiska dataskyddsstyrelsen skulle dock vilja behandla tre aspekter i samband med detta. För det första har medlingstjänsten inte offentliggjorts på den engelska versionen av PPC:s webbplats. För det andra är tjänsten endast tillgänglig via telefon och på japanska. Slutligen är medling endast ett frivilligt förfarande som inte leder till ett bindande avtal mellan parterna, vilket påverkar effektiviteten när det gäller de möjligheter till prövning som är tillgängliga för de registrerade[59].

134. Europeiska dataskyddsstyrelsen noterar slutligen att tonvikten i förslaget till beslut om adekvat skyddsnivå ligger på de rättsmedel som är tillgängliga genom civilrättsliga- och straffrättsliga förfaranden, men uppmärksammar inte att det finns **institutionella hinder mot rättstvister** i Japan, såsom rättegångskostnader (rättegångskostnader delas lika mellan käranden och svaranden, oavsett

[65] Oda H., Japanese Law, Oxford University Press (tredje upplagan), 2009, 439–440.
[58]https://www.ppc.go.jp/en/contactus/piinquiry/.
[59] Kojima T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004 och Menkel-Meadow C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003) (utgivare).

vilken part som vinner målet[60]), bristen på advokater i landet[61], det faktum att utländska advokater inte får tillämpa inhemsk lagstiftning samt krav vad gäller bevisbördan enligt skadeståndsrätten. Europeiska dataskyddsstyrelsen befarar att dessa faktorer – i praktiken – kan hindra enskildas tillgång till rättslig prövning och äventyra deras rätt att snabbt vidta rättsliga åtgärder utan orimliga kostnader.

135. Mot bakgrund av ovanstående **befarar Europeiska dataskyddsstyrelsen att det finns en risk för att enskilda personer i EU kan ha svårt att få tillgång till administrativ och rättslig prövning** och skulle därför välkomna om kommissionen kunde diskutera möjligheten att inrätta en onlinetjänst med PPC, i vart fall på engelska, **i syfte att ge stöd till och hantera klagomål från[62] enskilda personer i EU**. Dessutom skulle Europeiska dataskyddsstyrelsen välkomna en möjlighet att tillåta EU:s dataskyddsmyndigheter att fungera som mellanhänder för klagomål från registrerade från EU gentemot organisationer som är verksamma i Japan och PPC.

4 ANGÅENDE OFFENTLIGA MYNDIGHETERS TILLGÅNG TILL UPPGIFTER SOM ÖVERFÖRTS TILL JAPAN

136. Genom beslutet om adekvat skydd har kommissionen i syfte att erkänna att ”Japan säkerställer en adekvat skyddsnivå för personuppgifter som överförs från Europeiska unionen till näringsidkare som hanterar personuppgifter i Japan”, såsom anges i artikel 1 i förslaget till beslut om adekvat skyddsnivå. I enlighet med artikel 45.2 GDPR har kommissionen också analyserat begränsningar och skyddsåtgärder när det gäller offentliga myndigheters tillgång till personuppgifter. I detta kapitel ligger fokus på en bedömning av brottsbekämpande myndigheters och andra statliga organs tillgång till personuppgifter för nationell säkerhet. Europeiska dataskyddsstyrelsens analys grundas på bilaga II till förslaget till beslut om adekvat skyddsnivå, i vilken den japanska regeringen tillhandahåller en översikt över den relevanta rättsliga ramen, och den japanska lagstiftningen, i den utsträckning kommissionen har tillhandahållit dessa. Europeiska dataskyddsstyrelsen har därför mot bakgrund av det specifika sammanhanget vid denna bedömning tagit hänsyn till de delar av den japanska lagstiftningen som inte ingår i kommissionens bedömning, men är relevanta vid bedömningen av de villkor och skyddsåtgärder enligt vilka de japanska offentliga myndigheterna ges tillgång till personuppgifter som överförs från Europeiska unionen.

4.1 Tillgång till uppgifter i brottsbekämpningssyfte

4.1.1 Förfaranden för att få tillgång till uppgifter på det straffrättsliga området

137. I förslaget till beslut om adekvat skyddsnivå anges tre möjligheter enligt japansk lagstiftning för brottsbekämpande myndigheter att få tillgång till uppgifter i Japan:

4.1.1.1 Begäran om tillgång med ett domstolsbeslut

138. I förslaget till beslut om adekvat skyddsnivå anges att när det gäller tillgång för statliga myndigheter i Japan, och särskilt för brottsbekämpande myndigheter att begära tillgång till elektronisk bevisning i

[60] Wagatsuma (2012), *Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure* i Reimann (utgivare), Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice volym 11, s. 195–200.

[61] Enligt de senaste siffrorna uppgår antalet advokater i Japan till 38 980 (ungefär 290 advokater per miljon invånare [Japan Federation of Bar Association] (2017), White Paper on Attorneys, s. 8–9.

[62] I likhet med vad som anges i bilaga II till detta beslut om adekvat skyddsnivå för klagomål från EU-medborgare avseende tillgång till deras uppgifter från japanska offentliga myndigheter.

samband med brottsutredningar, krävs det alltid ett domstolsbeslut, såvida de inte använder förfarandet för frivilligt utlämnande av uppgifter – se nedan.

4.1.1.1.1 Krav på ”tillräcklig grund” samt att domstolsbeslut är nödvändiga och proportionerliga

139. Europeiska dataskyddsstyrelsen erkänner att enligt den japanska författningen måste all insamling av personuppgifter genom tvångsmedel grundas på ett domstolsbeslut. I förslaget till beslut om adekvat skyddsnivå anges närmare bestämt att det i samtliga fall av ”husrannsakan och beslag” krävs att det utfärdas ett domstolsbeslut för ”tillräcklig grund”. Enligt högsta domstolen anses en sådan grund endast föreligga om den berörda personen (den misstänkte eller tilltalade) anses ha begått ett brott och husrannsakan och beslag är nödvändiga för brottsutredningen. Kommissionen hänvisar i detta avseende till högsta domstolens dom av den 18 mars 1969, mål N. 100 (1968 (SHi)). Europeiska dataskyddsstyrelsen erinrar om att enligt EU-domstolens rättspraxis[63] kan endast en domstol, och inte exempelvis åklagare, godkänna insamling av i synnerhet trafik- och lokaliseringsuppgifter.

140. Mot bakgrund av EU-domstolens rättspraxis, enligt vilken tillgång till uppgifter kan kräva ett domstolsbeslut, som i målet Tele2, beklagar Europeiska dataskyddsstyrelsen att ingen ytterligare information har tillhandahållits för att det ska kunna bedömas hur kriterierna för att utvärdera om ett domstolsbeslut var nödvändigt (dvs. brottets allvarlighetsgrad och hur det begicks, det beslagtagna materialets värde och betydelse som bevismaterial, sannolikheten för att beslagtagna material ska gömmas eller förstöras, i vilken utsträckning beslaget orsakar nackdelar och andra relaterade villkor) och hur begreppet ”tillräcklig grund”, som härrör från författningen, tillämpas i praktiken. Därför uppmanar Europeiska dataskyddsstyrelsen kommissionen att övervaka om utfärdandet av domstolsbeslut i praktiken uppfyller de kriterier som fastställts av EU-domstolen.

4.1.1.1.2 Typer av brott för vilka domstolsbeslut kan utfärdas

141. Domstolsbeslut krävs endast när det genomförs en ”obligatorisk undersökning”. I princip kan dessa domstolsbeslut endast utfärdas i fall där en lagöverträdelse har ägt rum. I detta avseende noterar Europeiska dataskyddsstyrelsen den nyligen antagna ”lagen om bestraffning av organiserad brottslighet och kontroll av vinning av brott” av den 15 juni 2017, i samband med Japans anslutning till FN:s internationella konvention om gränsöverskridande organiserad brottslighet[64]. I avsaknad av en engelsk version av denna lagstiftning, och mot bakgrund av kravet i unionslagstiftningen att vissa uppgifter endast samlas in i samband med utredning, avslöjande eller lagföring av allvarliga brott[65], samt med hänsyn till de farhågor som framförts av flera kommentatorer, däribland FN:s särskilda rapportör Joseph Cannataci[66], avseende det breda tillämpningsområdet, vilket grundas på en definition av ”organiserad kriminell grupp” som enligt uppgift är vag och alltför bred, kan Europeiska dataskyddsstyrelsen inte dra slutsatsen att tillgången till elektronisk bevisning enligt den relevanta japanska lagstiftningen är begränsad till de tröskelvärden som fastställs i unionslagstiftningen.

142. Det är också värt att notera att den regionala polisen är behörig för vissa typer av brott och har sina särskilda polisförordningar. Europeiska dataskyddsstyrelsen har inte haft tillgång till de interna bestämmelser som är tillämpliga på den regionala polisen.

143. Enligt förslaget till beslut om adekvat skyddsnivå omfattas insamling av elektronisk information på det straffrättsliga området av den regionala polisens ansvarsområde.

---

[63] Se EU-domstolens domar i mål C-203/15, C-293/12 och C-594/12.
[64] Se: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.
[65] Se de förenade målen C-293/12 och C-594/12 samt mål C-203/15.
[66] FN:s särskilda rapportör för rätten till privatliv samt Graham Greenleaf, rättsforskare vid University of New South Wales.

4.1.1.2 Beslut om avlyssning

144. I bilaga II till förslaget till beslut om adekvat skyddsnivå anges att särskilda villkor för avlyssning av kommunikation föreskrivs i lagen om avlyssning i brottsutredande syfte. Denna lagstiftning tillhandahölls mycket sent, vilket medförde att någon djupgående analys inte var möjlig. Även om det tycks tillhandahållas många skyddsåtgärder inom denna rättsliga ram kan Europeiska dataskyddsstyrelsen inte bedöma om de villkor som föreskrivs i denna lagstiftning innehåller garantier som väsentligen motsvarar dem som krävs i EU, både i stadgan, såsom den tolkats av EU-domstolen, och i Europakonventionen, såsom den tolkats av Europadomstolen.

4.1.1.3 Förfarandet för ”frivilligt utlämnande” på grundval av kontrollformulär

145. Denna icke-obligatoriska form av samarbete ger de offentliga myndigheterna möjlighet att be personuppgiftsansvariga (med undantag för telekommunikationsoperatörer) att tillhandahålla uppgifter som de har tillgång till. Underlåtenhet att iaktta en sådan begäran kan inte verkställas. Det står inte klart vilka myndigheter som kan använda denna typ av förfarande, men det tycks vara begränsat till brottsutredande myndigheter.

4.1.1.3.1 Villkor för utfärdande av ”kontrollformulär”

146. Europeiska dataskyddsstyrelsen erkänner att Japans högsta domstol, med hänvisning till författningen, har fastställt begränsningar för användningen av ”frivilligt utlämnande”[67]. Det framgår av förslaget till beslut om adekvat skyddsnivå att de behöriga myndigheterna i praktiken endast kan begära ett ”frivilligt utlämnande” genom att utfärda ett ”kontrollformulär”. Det uppges endast vara tillåtet att skicka ett sådant ”kontrollformulär” som en del av en brottsutredning, vilket alltid förutsätter en konkret misstanke om att ett brott har begåtts. Sådana utredningar utförs i allmänhet av den regionala polisen, där begränsningarna enligt artikel 2.2 i polislagen är tillämpliga, vilket innebär att den ska vara relevant för polisens verksamhet. Europeiska dataskyddsstyrelsen efterfrågar dock ytterligare klargöranden vad gäller den konkreta utformningen av villkoren för utfärdandet av ett kontrollformulär (såsom rättspraxis som illustrerar tillämpningen av dessa kriterier), och förhållandet mellan förfarandet för frivilligt utlämnande av uppgifter och beslagtagande av uppgifter på grundval av ett domstolsbeslut. Det förefaller som om uppgifter som inte kunde inhämtas genom det frivilliga förfarandet fortfarande skulle kunna erhållas genom ett domstolsbeslut om det är nödvändigt för de utredande myndigheterna[68].

4.1.1.3.2 Tillgänglig rättspraxis avseende begränsningar av användningen av frivilligt utlämnande av uppgifter

147. De mål som det hänvisas till i förslaget till beslut om adekvat skyddsnivå[69] för att illustrera begränsningar av användningen av förfarandet för frivilligt utlämnande avser fall där den anklagade personen antingen fotograferades eller filmades direkt på allmän plats av polisen. De ger därför begränsad information om situationer där de behöriga myndigheterna kan begära att en personuppgiftsansvarig lämnar ut uppgifter, i synnerhet när det gäller de kriterier som anges i bilaga II avseende ”lämpliga metoder”, vilket verkar röra bedömningen av huruvida en frivillig undersökning är ”lämplig” eller rimlig för att uppnå syftet med undersökningen. Detsamma kan sägas om de allmänna kriterierna om ”huruvida det kan anses rimligt i enlighet med socialt accepterade konventioner” för att bedöma om de frivilliga undersökningarna är lagliga. Dessutom har den nationella polismyndigheten, som är den federala myndighet som ansvarar för alla frågor som rör kriminalpolisen, utfärdat instruktioner till den regionala polisen om ”korrekt användning av skriftliga

[67] Se bilaga II, s. 8.
[68] Se bilaga II, s. 7.
[69] Se bilaga II s. 8 – två beslut från högsta domstolen av den 24 december 1969 (1965 (A) nr 1187) och av den 15 april 2008 (2007 (A) nr 839).

förfrågningar i utredningsärenden”. Den ansvariga utredaren måste bland annat erhålla ett internt godkännande från en högre tjänsteman. Europeiska dataskyddsstyrelsen har inga uppgifter om huruvida dessa instruktioner är bindande. Europeiska dataskyddsstyrelsen konstaterar dock att användningen av detta förfarande måste vara proportionerligt eller nödvändigt.

4.1.1.3.3 Personuppgiftsansvarigas rättigheter och skyldigheter i samband med frivilligt utlämnande av uppgifter

148. Dessutom åligger det de personuppgiftsansvariga att ge samtycke till att lämna ut uppgifter (men det förefaller inte finnas någon skyldighet för dem att inhämta samtycke från registrerade eller att informera dem) om dessa förfrågningar inte strider mot andra rättsliga skyldigheter (såsom skyldigheter som hänför sig till konfidentialitet). Den rapport som kommissionen har tillhandahållit tyder på att efter en hög grad av efterlevnad har personuppgiftsansvariga börjat ta hänsyn till uppgiftsskyddet från sina kunder och har således börjat svara i mindre utsträckning på dessa förfrågningar.

149. Det är också oklart om de personuppgiftsansvariga har några incitament för att uppfylla förfrågningarna (till exempel om de erhåller någon fördel vid efterlevnad, eller om de är undantagna från lagföring, etc.). I synnerhet hänvisas inte till någon liknande princip som principen att ingen får vittna mot sig själv.

150. Europeiska dataskyddsstyrelsen välkomnar ytterligare information, i förekommande fall sifferuppgifter avseende antalet och typerna av förfrågningar samt avseende de svar som lämnats av de tillfrågade personuppgiftsansvariga. I avsaknad av rättspraxis och sifferuppgifter uppmanar Europeiska dataskyddsstyrelsen kommissionen att övervaka effektiviteten och hur detta förfarande tillämpas i praktiken.

151. Europeiska dataskyddsstyrelsen saknar emellertid rättspraxis och sifferuppgifter avseende detta förfarande för att kunna fastställa dessa faktorer. Utan ytterligare faktorer rörande praxis kan följaktligen Europeiska dataskyddsstyrelsen inte göra någon bedömning om effektiviteten och den konkreta tillämpningen av detta förfarande.

4.1.1.4 Slutsatser om förfarandena för tillgång till uppgifter i brottsbekämpande syfte

152. Sammanfattningsvis erkänner Europeiska dataskyddsstyrelsen att den princip enligt vilken behöriga myndigheter kan få obligatorisk tillgång till personuppgifter endast när detta är nödvändigt och proportionerligt i förhållande till syftet, och på grundval av ett domstolsbeslut, motsvarar de viktigaste grundläggande garantier som föreskrivs i unionslagstiftningen och enligt Europakonventionen. Mot bakgrund av ovanstående bedömning uppmanar Europeiska dataskyddsstyrelsen kommissionen att övervaka tillämpningsområdet för dessa åtgärder, omfattningen av förfarandet för frivilligt utlämnande av uppgifter och den regionala polisens tillämpning av denna princip och domstolarnas tillämpning i relevant rättspraxis samt att även övervaka om den japanska rättsliga ramen tillhandahåller sådana grundläggande garantier som EU-domstolen har fastställt på grundval av stadgan och Europadomstolen på grundval av Europakonventionen.

4.1.2 Tillsyn på det straffrättsliga området

153. I förslaget till beslut om adekvat skyddsnivå samt i bilaga II till nämnda beslut presenteras fyra typer av tillsyn som genomförs av polis, ministerier och offentliga myndigheter.

4.1.2.1 Rättslig tillsyn

4.1.2.1.1 I situationer där elektronisk information samlas in med tvångsmedel (husrannsakan och beslag)

154. I samtliga fall där elektronisk information samlas in med tvångsmedel (husrannsakan och beslag) är polisen enligt förslaget till beslut om adekvat skyddsnivå skyldig att i förväg inhämta ett domstolsbeslut. Det finns emellertid ett undantag från denna regel[70]. Enligt artikel 220.1 i straffprocesslagen får en åklagare, dennes biträde eller en kriminalpolistjänsteman som griper en misstänkt person göra en husrannsakan eller beslagta elektronisk information på platsen för gripandet. I sådana situationer finns det en möjlighet att domstolen kan underkänna dessa uppgifter som bevisning.

155. Europeiska dataskyddsstyrelsen är medveten om att det förekommer liknande undantag enligt unionslagstiftningen. Europeiska dataskyddsstyrelsen noterar att det inte alltid föreligger någon rättslig kontroll när elektronisk information samlas in med tvångsmedel, såsom anges i förslaget till beslut om adekvat skyddsnivå. I detta sammanhang hänvisar Europeiska dataskyddsstyrelsen till Europadomstolens rättspraxis beträffande rättsliga kontroller i efterhand.[71]

4.1.2.1.2 Vid förfrågningar om frivilligt utlämnande av uppgifter

156. Enligt förslaget till beslut om adekvat skyddsnivå föreligger inte någon förhandskontroll från domstol när det gäller begäran om frivilligt utlämnande av uppgifter. I ett sådant fall står den regionala polisen under åklagarmyndighetens tillsyn. I förslaget till beslut om adekvat skyddsnivå hänvisas till artiklarna 192.1 och 246 om ömsesidigt samarbete och samordning av åklagare, den regionala kommissionen för allmän säkerhet och kriminalpolistjänstemän samt utbyte av information mellan dem. Vidare hänvisas till artikel 193.1, enligt vilken åklagarmyndigheten kan ge nödvändiga instruktioner till kriminalpolisen samt fastställa normer för en rättvis utredning. Slutligen hänvisas det till artikel 194, enligt vilken den nationella eller regionala kommissionen för allmän säkerhet kan vidta disciplinära åtgärder mot kriminalpolisen för att de inte respekterar åklagarmyndigheten.

157. Europeiska dataskyddsstyrelsen erkänner genomförandet av ovannämnda åtgärder och den tillsyn av kriminalpolisen som genomförs av nationella och regionala kommissionen för allmän säkerhet (se nedan).

4.1.2.2 Tillsyn av polisen genom kommissionerna för allmän säkerhet

158. Enligt bilaga II till förslaget till beslut om adekvat skyddsnivå utövar två typer av kommissioner tillsyn över polisen. Båda har i syfte att säkerställa en demokratisk förvaltning och politisk neutralitet inom polisförvaltningen.

4.1.2.2.1 Tillsyn som utövas av den nationella kommissionen för allmän säkerhet

159. I bilaga II till förslaget till beslut om adekvat skyddsnivå hänvisas till den tillsyn som den nationella kommissionen för allmän säkerhet utövar över den nationella polismyndigheten. Polislagen innehåller en förteckning över de uppgifter som kommissionen har och från vilka dess tillsynsbefogenheter härstammar (se artikel 5).

160. Enligt artikel 4 i polislagen är den nationella kommissionen för allmän säkerhet inrättad under premiärministerns jurisdiktion och består av en ordförande och fem ledamöter. I artikel 7 fastställs vissa begränsningar för utnämningen av kommissionens ledamöter. Mandatperioden för kommissionens ledamöter är fem år och får endast förnyas en gång, såsom föreskrivs i artikel 8. Dessutom förefaller parlamentet ha stor makt över tillsättningen och avskedandet av

[70] Se bilaga II.
[71] Europadomstolen, Modestou mot Grekland, nr 51693/13.

kommissionsmedlemmarna, vilket säkerställer att den nationella kommissionen för allmän säkerhet är oberoende.

161. Sådana rättsliga bestämmelser stärker den politiska neutraliteten från den nationella kommissionen för allmän säkerhet.

4.1.2.2.2 Tillsyn som utövas av de regionala kommissionerna för allmän säkerhet

162. Den regionala polisen står under tillsyn av de regionala kommissionerna för allmän säkerhet som inrättats i varje region. Enligt artiklarna 2 och 36.2 i polislagen ansvarar de regionala kommissionerna för allmän säkerhet för ”skydd av enskildas rättigheter och frihet”. I artiklarna 38 och 42 i polislagen anges vilka skyldigheter de regionala kommissionerna för allmän säkerhet har. Dessa kommissioner ska även säkerställa att polisförvaltningen är demokratisk och politisk neutral, såsom föreskrivs i artikel 43.2, genom att hänskjuta enskilda fall till den regionala polisen när de anser att detta krävs i samband med en inspektion av den regionala polisens verksamhet eller försummelse från dess personal.

163. Det är emellertid oklart om dessa kommissioner har andra befogenheter än att kontrollera polisens beteende. Europeiska dataskyddsstyrelsen undrar om begreppet ”försummelse” omfattar olaglig tillgång till uppgifter och, i så fall, om dessa kommissioner kan beordra radering av uppgifter eller inte.

164. Vad gäller neutraliteten och oberoendet från de regionala kommissionerna för allmän säkerhet, så inrättas dessa kommissioner, såsom anges i förslaget till beslut om adekvat skyddsnivå[72], under den regionala guvernörens jurisdiktion. Guvernören utser ledamöter till kommissionen med godkännande från den regionala församlingen. Mandatperioden för ledamöterna i den regionala kommissionen för allmän säkerhet är tre år och kan förlängas upp till två gånger. I artikel 39 i polislagen föreskrivs begränsningar vad gäller utnämningen av medlemmarna. I förslaget till beslut om adekvat skyddsnivå hänvisas även till den lokala församlingens tillsyn av den regionala polisen, med hänvisning till artikel 100 i lagen om lokalt självstyre. Europeiska dataskyddsstyrelsen har emellertid inte erhållit denna rättsakt[73].

165. Enligt artikel 42.2 och 42.3 i polislagen ska dessutom ”[i]ngen ledamot av kommissionen [...] samtidigt tillhöra församlingen eller den personal som arbetar heltid vid lokala offentliga organ eller vara deltidsanställd såsom föreskrivs i artikel 28.5 första stycket i lagen om lokal offentlig förvaltning”.

166. Mot denna bakgrund och med beaktande av samarbetet mellan de regionala kommissionerna för allmän säkerhet och den nationella kommissionen för allmän säkerhet instämmer Europeiska dataskyddsstyrelsen med förslaget till beslut om adekvat skyddsnivå och välkomnar neutraliteten och oberoendet från ledamöterna i de regionala kommissionerna för allmän säkerhet. Såsom Europeiska dataskyddsstyrelsen har förstått har de regionala kommissionerna för offentlig säkerhet endast befogenhet att utreda polisens agerande och saknar andra tillsynsbefogenheter, inbegripet radering av uppgifter som den regionala polisen har samlat in. Det tycks därför krävas ytterligare klargöranden om huruvida tillsynen från de regionala kommissionerna för allmän säkerhet är tillräcklig enligt de normer som fastställs i unionslagstiftningen.

4.1.2.2.3 Tillsyn som utövas av parlamentet

167. I förslaget till beslut om adekvat skyddsnivå[74] och i bilaga II[75] tillhandahålls viss information om den tillsyn som parlamentet utför i förhållande till regeringen, bland annat beträffande lagligheten från

[72] Se förslaget till beslut om adekvat skyddsnivå s. 31.
[73] Se förslaget till beslut om adekvat skyddsnivå s. 33.
[74] Se förslaget till beslut om adekvat skyddsnivå s. 30.
[75] Se bilaga II, s. 12.

polisens insamling av uppgifter. I båda hänvisas till artikel 62 i författningen, enligt vilken parlamentet kan begära framtagande av handlingar och vittnesuppgifter. I båda hänvisas också till rättsliga bestämmelser från lagen om parlamentet, särskilt artikel 104 beträffande parlamentets befogenheter, samt artikel 74 beträffande ingivandet av skriftliga frågor som kansliet ska besvara skriftligen inom sju dagar i enlighet med artikel 75. I förslaget till beslut om adekvat skyddsnivå anges även följande: ”Parlamentets roll när det gäller att utöva tillsyn över den verkställande makten stöds av rapporteringsskyldigheter, till exempel i enlighet med artikel 29 i lagen om avlyssning”.

168. Europeiska dataskyddsstyrelsen erkänner parlamentets delaktighet vid tillsynen av regeringen och polisen beträffande lagligheten från insamlingen av uppgifter.

4.1.2.2.4 Tillsyn som utövas av den verkställande makten

169. Enligt bilaga II i förslaget till beslut om adekvat skyddsnivå är ministern eller chefen för varje ministerium eller byrå, ansvarig för tillsyn och verkställighet på grundval av lagen om skydd av personuppgifter som innehas av förvaltningsorgan (nedan kallad *APPIHAO*)[76]. Å andra sidan har ministern för inrikes frågor och kommunikation (nedan kallad inrikesministern) utredningsbefogenheter när det gäller tillsynen av andra ministeriers efterlevnad av APPIHAO, däribland justitieministern för polisen, såsom anges i förslaget till beslut om adekvat skyddsnivå[77].

170. Ministern kan begära att chefen för ett förvaltningsorgan inger material och förklaringar beträffande hanteringen av personuppgifter från det berörda förvaltningsorganet på grundval av artikel 50 APPIHAO. Ministern kan begära en översyn av åtgärderna när det finns misstanke om överträdelse eller felaktig tillämpning av lagen samt avge yttranden avseende hanteringen av personuppgifter från det berörda förvaltningsorganet i enlighet med artiklarna 50 och 51 APPIHAO.

171. I förslaget till beslut om adekvat skyddsnivå och i bilaga II hänvisas även till även inrättandet av 51 heltäckande informationscentrum som ska ”säkerställa ett smidigt genomförande av denna lag” i enlighet med artikel 47 APPIHAO. Europeiska dataskyddsstyrelsen noterar att den roll och de befogenheter som dessa informationscenter har inte förklaras närmare i APPIHAO, men att vissa preciseringar görs i förslaget till beslut om adekvat skyddsnivå.

172. Europeiska dataskyddsstyrelsen välkomnar således att inrikesministern utövar en verkställande tillsyn när det gäller ministeriernas och förvaltningsorganens efterlevnad av APPIHAO.

173. Som en slutsats fastställs standarder och garantier i unionslagstiftningen och i Europakonventionen, genom rättspraxis från deras respektive domstolar, enligt vilka tillsynen måste vara fullständig, neutral och oberoende. Europeiska dataskyddsstyrelsen noterar att PPC inte har tillsynsbefogenheter i frågor som rör brottsbekämpning. Om den tillsyn som genomförs av parlamentet och den nationella och regionala säkerhetskommissionen anses vara neutral och oberoende, krävs dessutom ytterligare klargöranden om tillsynsbefogenheten från de regionala kommissionerna för allmän säkerhet.

4.1.3 Prövning inom det straffrättsliga området

174. I förslaget till beslut om adekvat skyddsnivå, i förening med bilaga II, presenteras flera möjligheter för enskilda att framföra klagomål, både till oberoende myndigheter och domstolar.

175. Dessa möjligheter och de centrala inslagen i dessa förfaranden som härrör från den tillgängliga dokumentationen presenteras nedan, efter en kort översikt över de tillgängliga rättigheterna för att

[76] Se bilaga II s. 10.
[77] Se bilaga II s. 11.

klargöra vad de registrerade kan förvänta sig av offentliga myndigheter inom ramen för behandlingen av uppgifter vid straffrättsliga förfaranden.

4.1.3.1 Tillgängliga rättigheter för registrerade i samband med straffrättsliga förfaranden

176. För att erhålla prövning krävs det att registrerade har rättigheter enligt lag för att det ska kunna hävdas att dessa inte har respekterats. Därför har Europeiska dataskyddsstyrelsen även bedömt de tillgängliga rättigheterna i samband med de straffrättsliga förfaranden som presenterades i förslaget till beslut om adekvat skyddsnivå.

4.1.3.1.1 Allmänna begränsningar av de registrerades rättigheter enligt APPIHAO

177. I sitt förslag till beslut om adekvat skyddsnivå hänvisar kommissionen till och förlitar sig på allmänna principer för uppgiftsskydd som offentliga myndigheter är skyldiga att iaktta när de samlar in personuppgifter. Dessa principer beskrivs också närmare i bilaga II, varför Europeiska dataskyddsstyrelsen har beslutat att även lämna synpunkter på dem.

178. När det gäller tillgängliga rättigheter noterar Europeiska dataskyddsstyrelsen att enligt bilaga II i förslaget till beslut om adekvat skyddsnivå är vissa av de allmänna rättigheterna för registrerade i samband med förvaltningsorganens behandling av uppgifter även tillgängliga i samband med brottsutredningar. Det finns dock ytterligare begränsningar vad gäller insamling och ytterligare hantering av personuppgifter i detta sammanhang som följer av APPIHAO.

179. Dessa begränsningar, som förefaller gälla både för uppgifter som samlas in på grundval av ett domstolsbeslut och på grundval av ett kontrollformulär i samband med frivilligt utlämnande av uppgifter, medför att det uppkommer ett flertal frågor.

180. Vad gäller principen om ändamålsbegränsning kan förvaltningsorgan – även om de i princip är skyldiga att specificera det syfte för vilket de lagrar personuppgifter och inte får lagra dem utöver vad som är nödvändigt för att uppnå syftet med den specificerade användningen – ändra syftet om det är ”vad som rimligen kan anses vara lämpligt för det ursprungliga ändamålet”.

181. I APPIHAO föreskrivs även principen att uppgifter inte ska lämnas ut. Enligt denna princip får en anställd inte lämna ut de personuppgifter som erhållits till en annan person utan berättigade skäl eller använda sådan information för ett oberättigat ändamål. Emellertid tillhandahålls inte någon ytterligare information beträffande tolkningen av vad som omfattas av ”berättigade skäl” eller ”oberättigade ändamål”, vilket gör att denna bedömning kräver ytterligare klargöranden.

182. I artikel 8.1 APPIHAO föreskrivs även ett förbud mot att använda eller lämna ut uppgifter ”om inte annat föreskrivs i lagar och andra författningar”. Även om denna bestämmelse i princip är förenlig med den skyddsnivå som garanteras enligt unionslagstiftningen saknar Europeiska dataskyddsstyrelsen ytterligare information gällande i vilken utsträckning tillsyn eller kontroll utövas när ett utlämnande föreskrivs i lagar eller andra författningar. Enligt artikel 8.2 föreskrivs dessutom ytterligare undantag från denna regel om ”ett sådant exceptionellt utlämnande av uppgifter sannolikt inte orsakar omotiverad skada för den registrerades eller en tredje parts rättigheter och intressen”. I avsaknad av ytterligare kriterier i detta hänseende krävs det ett förtydligande om detta undantag, som bygger på det oklara begreppet ”omotiverad” skada, är tillräckligt restriktivt.

183. I artikel 9 APPIHAO föreskrivs slutligen ytterligare begränsningar av ändamålet eller användningsmetoden eller eventuella andra begränsningar som ska införas av chefen för ett förvaltningsorgan, om lagrade personuppgifter tillhandahålls en annan person. Eftersom begreppen ”eventuella andra nödvändiga begränsningar” och ”tillhandahålls en annan person” är mycket breda,

ger dessa ytterligare begränsningar av de registrerades rättigheter upphov till oro i avsaknad av ytterligare förtydliganden om tillämpningsområdet för denna bestämmelse.

184. Även om Europeiska dataskyddsstyrelsen är fullt medveten om att rätten till tillgång och andra principer för uppgiftsskydd också är begränsade i straffrättsliga förfaranden enligt unionslagstiftningen. Ytterligare skyddsåtgärder tillhandahålls när sådana begränsningar förutses, bland annat genom övervakning, tillsyn och prövning. I avsaknad av tillräcklig rättspraxis beträffande dessa begränsningar eller ytterligare kriterier för att klargöra tillämpningsområdet för dessa bestämmelser kan Europeiska dataskyddsstyrelsen inte bedöma om dessa begränsningar av de registrerades rättigheter är begränsade till vad som anses vara strikt nödvändigt och proportionerligt enligt unionslagstiftningen, och därför är väsentligen likvärdiga med de rättigheter som registrerade har i EU.

4.1.3.1.2 Ytterligare begränsningar av rättigheterna i APPIHAO som härstammar från straffprocesslagen och regionpolisförordningarna

185. Europeiska dataskyddsstyrelsen noterar att även om APPIHAO förefaller vara tillämplig på all behandling som utförs av förvaltningsorgan i Japan föreligger det vissa viktiga begränsningar av de registrerades rättigheter som härstammar från särskild lagstiftning. Särskilt föreskrivs i artikel 53.2 i straffprocesslagen[78] att ”personuppgifter som har registrerats i handlingar som rör rättegångar och beslagtagna varor” undantas från tillämpningsområdet för de individuella rättigheterna i kapitel IV i APPIHAO. Konkret tolkar Europeiska dataskyddsstyrelsen detta som att de registrerade inte åtnjuter någon rätt till information, åtkomst, rättelse eller radering av personuppgifter i handlingar som rör rättegångar och beslagtagna varor i samband med straffrättsliga förfaranden.

186. Vad gäller dessa begränsningar uppfattar Europeiska dataskyddsstyrelsen att de är tillämpliga på uppgifter som samlas in såväl på grundval av domstolsbeslut som inom ramen för frivilligt utlämnande av uppgifter via kontrollformulär (se nedan). Den rättsliga grunden för de två förfarandena för att få tillgång till uppgifter (genom domstolsbeslut och genom kontrollformulär) som föreskrivs i straffprocesslagen. Artikel 53.2 i nämnda lag förefaller gälla för båda typerna av insamling. Eftersom artikel 53.2 hänvisar till ”beslagtagna” varor skulle det dock kunna klargöras om begränsningarna av de rättigheter som föreskrivs i denna bestämmelse också gäller i samband med frivilligt utlämnande av uppgifter.

187. Tyvärr har Europeiska dataskyddsstyrelsen inte erhållit de förordningar från den regionala polisen som uppges skydda personuppgifter, rättigheter och skyldigheter som är likvärdiga med APPIHAO. Såväl på grund av oklarheten när det gäller hur APPIHAO ska tolkas som att de regionala polisförordningarna inte är tillgängliga, anser Europeiska dataskyddsstyrelsen att det är osäkert om de rättigheter som enskilda personer beviljas i detta sammanhang och de extra tillsyns- och/eller prövningsmekanismerna är tillräckliga för att kompensera för avsaknaden av rättigheter.

4.1.3.2 Prövning genom oberoende myndigheter

4.1.3.2.1 Administrativ prövning

188. Europeiska dataskyddsstyrelsen noterar att de förvaltningsorgan som samlar in uppgifter, såsom den regionala polisen, är behöriga att behandla förfrågningar från enskilda personer om deras – begränsade – rättigheter med avseende på uppgifter om dem som samlas in vid brottsutredningar (se ovan avseende de tillgängliga rättigheterna), vilket verkar omfatta både insamling av uppgifter som grundar sig på ett domstolsbeslut och kontrollformulär. Rent konkret förefaller dessa rättigheter vara

[78] Tillgänglig här: http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 samt hänvisning i bilaga II till förslaget till beslut om adekvat skyddsnivå, fotnot 25.

begränsade till allmänna principer, såsom behovet av att lagra uppgifter, i samband med ändamålet (se artikel 3.1 APPIHAO), principen om ändamålsbegränsning (artikel 4) eller uppgifternas korrekthet (artikel 5), samtidigt som individuella rättigheter såsom rätten till information, tillgång, rättelse eller radering inte är tillämpliga på personuppgifter som registrerats i handlingar som rör rättegångar och beslagtagna varor[79]. Europeiska dataskyddsstyrelsen välkomnar denna möjlighet även om dessa organ inte kan anses vara oberoende och således tillhandahålla oberoende prövning eller tillsyn. Europeiska dataskyddsstyrelsen betonar dock att klagomål som inges i detta sammanhang är begränsade till de mycket få rättigheter som de registrerade har mot bakgrund av de begränsningar av rättigheter som föreskrivs i APPIHAO.

189. Eftersom ”personuppgifter som registrerats i handlingar som rör rättegångar och beslagtagna varor” enligt artikel 53.2 i straffprocesslagen undantas från tillämpningsområdet för de individuella rättigheterna i kapitel IV i APPIHAO, är möjligheterna att begära tillgång till personuppgifter också begränsade till de förfaranden som föreskrivs i andra bestämmelser i straffprocesslagen. Det förefaller som om endast brottsoffer, misstänkta eller tilltalade kan agera i detta sammanhang, beroende på i vilket skede det straffrättsliga förfarandet befinner sig. Europeiska dataskyddsstyrelsen är därför oroad över att de registrerade inte har någon allmän rätt att få tillgång till och/eller rätta eller radera uppgifter enligt japansk rätt i samband med straffrättsliga förfaranden, och att alla tillgängliga möjligheter till prövning antingen hänför sig till ett brottsoffer (i vilket fall personen sannolikt känner till att dennes uppgifter har samlats in) eller en misstänkt eller tilltalad, eller bevisning av en skada. Registrerade bör emellertid även ha rätt att få tillgång till sina uppgifter och eventuellt få sina uppgifter rättade eller raderade när de inte lidit någon skada (men en sådan skada är möjlig) och/eller om de varken är brottsoffer, misstänkta eller tilltalade, utan till exempel vittnen.

4.1.3.2.2 Administrativ prövning genom de regionala kommissionerna för allmän säkerhet

190. De regionala kommissionerna för allmän säkerhet förefaller dessutom vara behöriga att behandla klagomål. Enligt artikel 79 i polislagen, som förslaget till beslut om adekvat skyddsnivå hänvisar till, kan enskilda personer framföra klagomål mot olagligt eller olämpligt agerande från en polistjänsteman vid utövningen av tjänsten.

191. Europeiska dataskyddsstyrelsen önskar ett klargörande om en ”olaglig” behandling av personuppgifter kan klassificeras som ”ett olagligt eller felaktigt agerande från en polistjänsteman” och avseende det styrkande av en nackdel som förefaller krävas från den registrerade. I meddelandet från nationella polismyndigheten till polisen och den nationella kommissionen för allmän säkerhet om korrekt handläggning av klagomål avseende polisens tjänsteutövning begränsas klagomålen till konkreta påståenden om ”korrigering av en specifik nackdel till följd av ett olagligt eller olämpligt beteende, eller underlåtenhet att vidta nödvändiga åtgärder, av en polistjänsteman vid dennes utövande av sin tjänst” och möjligheten att ”inge klagomål/anmäla missnöje mot en polistjänsteman för felaktig tjänsteutövning”. Det klargörs uttryckligen att ”klagomål mot underlåtenhet från en polistjänsteman att fullgöra sina skyldigheter i frågor som inte anses falla under en polistjänstemans uppdrag, och även de som uttrycker en allmän åsikt eller ett förslag som inte direkt påverkar den klagande parten själv, ska vara uteslutna”.

192. När det gäller processuella krav för att inge klagomål, noterar Europeiska dataskyddsstyrelsen att även om de måste inges skriftligen, tillhandahålls bistånd för att skriva klagomålet enligt japansk rätt i detta sammanhang, även för utlänningar. Dessutom förefaller den japanska regeringen även ha ålagt PPC skyldigheten att bistå registrerade från EU när det gäller att hantera och lösa klagomål på detta

[79] Se ovan angående de begränsningarna i APPIHAO och se i synnerhet artikel 53.2 i straffprocesslagen (som inte har tillhandahållits men som bilaga II till förslaget till beslut om adekvat skyddsnivå hänvisar till i fotnot 25).

område, vilket Europeiska dataskyddsstyrelsen välkomnar. Europeiska dataskyddsstyrelsen betonar att den i detta sammanhang uppfattar att PPC endast kommer att fungera som kontaktpunkt mellan registrerade från EU och de behöriga myndigheterna i Japan.

193. I de situationer som anges i artikel 79.2 i polislagen, som omfattar situationen där klagandens hemvist är okänd, ska resultaten från den regionala kommissionen för allmän säkerhet inte meddelas. Europeiska dataskyddsstyrelsen erkänner att hänvisningen till hemvisten inte innebär att registrerade i EU i samtliga fall därför skulle vara uteslutna från att erhålla meddelande om resultaten av deras klagomål på grund av att de inte är bosatta i Japan.

4.1.3.2.3 Särskild mekanism som hänvisar till PPC

194. Mot bakgrund av de resultat som beskrivs ovan välkomnar Europeiska dataskyddsstyrelsen att den japanska regeringen och EU-kommissionen har kommit överens om en ytterligare mekanism för prövning som ger enskilda personer i EU en ytterligare möjlighet till rättslig prövning i Japan, genom vilka enskilda personer även kan väcka talan mot olagliga eller olämpliga utredningar från offentliga myndigheter. Europeiska dataskyddsstyrelsen noterar också och välkomnar att ansökningarna kan inges till PPC i stället för till en annan offentlig tjänsteman, vilket innebär att PPC:s behörighet utvidgas så att en även omfattar brottsbekämpning och nationell säkerhet.

195. Vid analysen av den nya mekanismen har Europeiska dataskyddsstyrelsen främst försökt förstå vilka befogenheter PPC har i detta sammanhang.

196. Även om språket inte är helt klart, drar Europeiska dataskyddsstyrelsen slutsatsen att den ytterligare prövningsmekanismen inte kräver någon ”ställning” i den meningen att sökanden inte behöver visa att dennes personuppgifter sannolikt har varit föremål för övervakning från en japansk myndighet. Europeiska dataskyddsstyrelsen vill emellertid ändå begära en bekräftelse från kommissionen.

197. I linje med sin bedömning av ombudsmansmekanismen, som inrättades inom ramen för skölden för skydd av privatlivet, betonar Europeiska dataskyddsstyrelsen behovet av effektiva befogenheter för adressaten från begäran, i detta fall PPC, för att prövningsmekanismen ska anses vara väsentligen likvärdig med ett effektivt rättsmedel i den mening som avses i artikel 47 i stadgan.

198. När den japanska regeringen redogjorde för prövningsmekanismen hänvisade den till artiklarna 6, 61 ii och 80 i personuppgiftslagen och har fastställt dessa befogenheter i bilaga II. Europeiska dataskyddsstyrelsen uppfattar det som att det förfarande som beskrivs i bilaga II specificerar eller utvidgar PPC:s befogenheter, eftersom språket i artiklarna 6, 61 ii och 80 i personuppgiftslagen är ganska vagt och allmänt. I den mån bilaga II specificerar eller utvidgar PPC:s befogenheter ber Europeiska dataskyddsstyrelsen om ett klargörande huruvida de övriga japanska statliga organ är bundna av dessa.

199. På grundval av förfarandet i bilaga II konstaterar Europeiska dataskyddsstyrelsen att de behöriga offentliga myndigheterna i Japan är skyldiga att samarbeta med PPC, ”bland annat genom att förse dem med nödvändig information och relevant material, så att PPC kan bedöma om insamlingen eller den efterföljande användningen av personuppgifter har skett i enlighet med tillämpliga regler”. Vid bedömningen av hur effektivt systemet är, är det således viktigt att än en gång hänvisa till de befogenheter som de behöriga myndigheter har med vilka PPC samarbetar. Europeiska dataskyddsstyrelsen tolkar det som att dessa befogenheter inte utvidgas genom försäkringarna i bilaga II.

200. Europeiska dataskyddsstyrelsen noterar också att om en överträdelse av reglerna har fastställt ”omfattar samarbetet mellan de berörda offentliga myndigheterna och PPC skyldigheten att rätta till

överträdelsen", vilket uttryckligen omfattar radering av de uppgifter som samlats in i strid med de tillämpliga bestämmelserna. Europeiska dataskyddsstyrelsen drar slutsatsen att den behöriga myndighetens skyldigheter härrör från "samarbetet med PPC", snarare än från ett beslut från PPC.

201. Slutligen kommer PPC att informera den sökande om "resultatet av utvärderingen, inbegripet i tillämpliga fall de eventuella korrigerande åtgärder som vidtagits." Dessutom kommer PPC att informera den sökande om "möjligheten att begära en bekräftelse av bedömningen från den behöriga offentliga myndigheten och om den myndighet till vilken en sådan begäran om bekräftelse ska göras."

202. Dessutom har PPC åtagit sig att bistå den sökande genom att vidta ytterligare åtgärder enligt japansk lagstiftning, om den sökande är missnöjd med resultatet av förfarandet.

203. Mot bakgrund av behovet av en effektiv prövningsmekanism som är väsentligen likvärdig med EU:s standarder anser Europeiska dataskyddsstyrelsen emellertid att det är oklart om PPC har några andra specifika befogenheter än att utvärdera om insamlingen eller den efterföljande användningen av personuppgifter har ägt rum i enlighet med tillämpliga regler och uppmana de behöriga myndigheterna att använda sina respektive befogenheter och hantera klagomål som PPC vidarebefordrat till dem. Om PPC endast fungerar som en kontaktpunkt för enskilda personer i EU anser Europeiska dataskyddsstyrelsen att detta inte är tillräckligt för att tillhandahålla en effektiv prövningsmekanism som är väsentligen likvärdig med EU:s standarder. Europeiska dataskyddsstyrelsen uppmanar därför kommissionen att klargöra de frågor som tas upp i detta underkapitel, i synnerhet om och på vilket sätt mekanismen utvidgar de behöriga myndigheternas skyldigheter, hur de är bundna av den och hur PPC på ett effektivt sätt kan säkerställa efterlevnaden och inte bara fungera som en kontaktpunkt för enskilda personer i EU.

4.1.3.3 Rättslig prövning

4.1.3.3.1 Kvasimekanism för klagomål

204. Det så kallade "kvasiförfarandet för klagomål" gör det möjligt att vidta åtgärder mot obligatorisk insamling av information som grundas på ett domstolsbeslut för att upphäva eller ändra ett olagligt beslag.

205. Denna möjlighet innebär att personen känner till vilka uppgifter som beslagtas. Såsom Europeiska dataskyddsstyrelsen uppfattar det underrättas den registrerade inte om förfarandet för insamling av uppgifter som grundas på ett domstolsbeslut. Vidare förstår Europeiska dataskyddsstyrelsen också att ett frivilligt utlämnande av uppgifter inte innebär att företag har en skyldighet att informera de registrerade om förfrågningar som mottagits och uppfyllts. Det framhålls i bilaga II att "en sådan utmaning kan åstadkommas utan att personen behöver vänta på att ärendet avslutas", är det i praktiken, med undantag för domstolsbeslut som medger avlyssning, för vilka anges att det föreskrivs ett anmälningskrav i lag[80]. I praktiken förefaller denna möjlighet emellertid först vara tillgänglig när den registrerade har fått kännedom om insamlingen genom en talan som väckts mot honom eller henne.

4.1.3.3.2 Förbudsföreläggande

206. Enskilda kan dessutom också väcka civilrättslig talan vid domstol för att erhålla en radering av uppgifter som samlats in vid ett straffrättsligt förfarande (s.k. förbudsföreläggande) eller för att få skadestånd.

[80] Artikel 23 i lagen om avlyssning nämns på sidan 33 i förslaget till beslut om adekvat skyddsnivå. Europeiska dataskyddsstyrelsen har emellertid inte erhållit denna text och kan därför inte bedöma i vilken utsträckning denna anmälningsskyldighet är tillämplig och i vilka situationer den kan vara begränsad.

207. När det gäller skadestånd noterar Europeiska dataskyddsstyrelsen att förfarandet förefaller vara begränsat till situationer där en offentlig tjänsteman, rättsstridigt och genom försummelse (uppsåtligen eller av oaktsamhet) har vållat den berörda personen skada i sin tjänsteutövning. Enligt vad Europeiska dataskyddsstyrelsen förstår förefaller skadan omfatta ideell skada. Det anges dock inte mer i detalj vilka beviskrav som åligger den enskilda personen vad gäller skadan. Europeiska dataskyddsstyrelsen har inte kunnat göra någon bedömning av rättspraxis avseende beviljande av ersättning och kan därför inte bedöma om denna möjlighet utgör ett effektivt rättsmedel vid skada.

208. När det gäller talan om förbudsföreläggande konstaterar Europeiska dataskyddsstyrelsen även att den enskilde för att väcka talan först måste vara medveten om att dennes uppgifter har samlats in och att de fortfarande lagras. Mot bakgrund av den begränsade informationen och tillgången till information för enskilda personer i samband med brottsutredningar och straffrättsliga förfaranden förefaller därför förfarandets effektivitet också vara ganska begränsad.

4.1.3.4 Sammantagen bedömning av möjligheterna till prövning

209. Efter bedömningen av alla möjligheter till rättslig prövning för enskilda enligt japansk lag och för registrerade från EU vid PPC, välkomnar Europeiska dataskyddsstyrelsen den särskilda tvistlösningsmekanismen som omfattar PPC. Den har ett mervärde för registrerade i EU, särskilt eftersom den gör det möjligt för dem att förstå vilka möjligheter som är tillgängliga för att erhålla prövning och/eller ersättning, samt att lägga fram sina förfrågningar i enlighet med de processuella krav som föreskrivs i japansk lagstiftning. Det krävs emellertid ytterligare klargöranden, i synnerhet om och på vilket sätt mekanismen utvidgar de behöriga myndigheternas skyldigheter, hur de är bundna av den, och hur PPC kan säkerställa effektiv efterlevnad, i syfte att säkerställa att denna nya mekanism tillhandahåller effektiv prövning.

210. Denna bedömning visar att det inte finns någon mekanism för prövning i japansk lagstiftning som gör det möjligt att få tillgång till, rätta eller radera uppgifter för registrerade som inte är brottsoffer, misstänkta eller tilltalade i samband med ett brottmålsförfarande, till exempel för att rätta till olaglig insamling eller lagring av deras uppgifter. Den visar också att alla mekanismer och förfaranden för prövning och ersättning som är tillgängliga enligt japansk lagstiftning för brottsoffer, misstänkta eller tilltalade förutsätter kännedom om insamlingen av uppgifter, vilket verkar vara begränsat i praktiken, eftersom begränsade rättigheter till tillgång och information tillhandahålls. Dessutom förefaller det krävas ytterligare förtydliganden vad gäller påvisandet av ett olagligt handlande från myndigheternas sida, i synnerhet huruvida ett sådant beteende omfattar all olaglig behandling av personuppgifter eller skada som den enskilde lider.

211. Utan ytterligare dokumentation och element hyser Europeiska dataskyddsstyrelsen därför oro över huruvida prövning enligt japansk lagstiftning och enligt förslaget till beslut om adekvat skyddsnivå är tillräckligt effektiv jämfört med standarderna i unionslagstiftningen.

4.2 Åtkomst för ändamål som rör nationell säkerhet

4.2.1 Kontrollens omfattning

212. I förslaget till beslut om adekvat skyddsnivå inleds kapitlet om ”japanska myndigheters tillgång till och användning för nationella säkerhetsändamål” med ett allmänt uttalande, i linje med den japanska regeringens försäkran i bilaga II, enligt vilken det inte i någon japansk lagstiftning föreskrivs och således tillåter ”obligatoriska framställningar om information eller ”administrativa avlyssning” utanför brottsutredningar”. Avslutningsvis anges att ”av nationella säkerhetsskäl kan endast information erhållas från en informationskälla som är tillgänglig för var och en eller genom ett frivilligt utlämnande av uppgifter. Detta utesluter all hemlig övervakningsverksamhet på detta område. Näringsidkare som

tar emot en begäran om frivilligt samarbete (i form av utlämnande av elektronisk information) har inte någon lagstadgad skyldighet att tillhandahålla sådan information."[81]

213. Inom dessa gränser anges fyra statliga organ som har befogenhet att samla in elektronisk information som innehas av japanska näringsidkare av nationella säkerhetsskäl. När det gäller försvarsministeriet, som utgör en av dessa fyra enheter, anges att det "endast har befogenhet att samla in (elektronisk) information genom frivilligt utlämnande av uppgifter".[82]

214. Vid sin bedömning av den allmänna utformningen av insamling av uppgifter av nationella säkerhetsskäl vill Europeiska dataskyddsstyrelsen erinra om den första av de fyra så kallade "grundläggande garantierna", enligt vilken "behandlingen bör grundas på tydliga, exakta och tillgängliga regler"[83]. Mer specifikt har Europadomstolen varit mycket tydlig med att övervakningsprogram endast "föreskrivs i lag" om kontrollåtgärderna "grundas på en intern föreskrift". Nämnda domstol har klargjort att det för en förenlighet med rättsstatsprincipen krävs att den lagstiftning i vilken åtgärden tillåts är tillgänglig och förutsebar vad gäller dess effekter. Med hänvisning till risken för godtycklighet har domstolen krävt "tydliga och detaljerade bestämmelser om hemliga övervakningsåtgärder", vilka är "tillräckligt tydliga för att ge medborgarna en tillräcklig indikation på under vilka omständigheter och under vilka förutsättningar offentliga myndigheter har rätt att vidta sådana åtgärder".[84]

215. För att dessa grundläggande garantier ska kunna tillämpas på det japanska rättssystemet är Europeiska dataskyddsstyrelsen inte bara medveten om att stater har ett stort utrymme för skönsmässig bedömning när det gäller frågor som rör nationell säkerhet, vilket har erkänts av Europadomstolen. De nationella säkerhetsbefogenheterna speglar också staternas historiska erfarenheter. Europeiska dataskyddsstyrelsen förstår således att de japanska nationella underrättelsetjänsterna efter andra världskriget har erhållit mer begränsade befogenheter än i andra stater, vilket den japanska regeringen framhåller.

216. Såsom Europeiska dataskyddsstyrelsen tolkar förslaget till beslut om adekvat skyddsnivå, i linje med den japanska regeringens försäkringar, driver japanska statliga organ inte program som i strategiskt hänseende eller i stor utsträckning övervakar kommunikation (via internet). Såsom påpekas ovan har den japanska regeringen lämnat försäkringar genom ett brev som är underskrivet av justitieministern att "av nationella säkerhetsskäl får information endast erhållas från en informationskälla som är tillgänglig för var och en eller genom ett frivilligt utlämnande av uppgifter".

217. När det gäller försvarsministeriets rättsliga grund konstaterar Europeiska dataskyddsstyrelsen att förslaget till beslut om adekvat skyddsnivå innehåller allmän information om dess befogenheter och hänvisar till dess uppdrag att "genomföra tillhörande verksamhet i syfte att säkerställa nationell fred och oberoende, och nationens säkerhet". Europeiska dataskyddsstyrelsen har inte erhållit någon engelsk översättning av den rättsliga grunden.

218. Samtidigt har Europeiska dataskyddsstyrelsen kännedom om rapporter som publicerats i olika medier som tyder på att direktoratet för signalspaning vid det japanska försvarsministeriet driver övervakningsprogram[85]. I rapporten hävdas också att det japanska försvarsministeriet har "erkänt att

[81] Beslut om adekvat skyddsnivå, punkt 151.
[82] Beslut om adekvat skyddsnivå, punkt 153.
[83] WP29, WP 237: Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (ej översatt till svenska).
[84] Se t.ex. Big Brother Watch m.fl. mot Förenade kungariket, punkt 305.
[85] I maj 2018 publicerade den nätbaserade tidningen "The Intercept" en rapport med titeln "The untold story of Japan's secret spy agency".

Japan har ”kontor i hela landet ” som avlyssnar kommunikation” och att de ”är inriktade på militär verksamhet och it-hot” och ”inte samlar in uppgifter från allmänheten”. Det senare uttalandet (att försvarsministeriet inte samlar in information om allmänheten) utgör en del av det nya uttalandet från den japanska regeringen.

219. Där uppges att den japanska regeringen i en skrivelse undertecknad av justitieministern har bekräftat att försvarsministeriet inte samlar in information om allmänheten.

220. Det ingår inte i Europeiska dataskyddsstyrelsens uppdrag att göra en allmän bedömning av den japanska regeringens möjligheter till övervakning. Sådana åtgärder är endast viktiga för bedömningen om de är relevanta för överföring av personuppgifter mellan EU och Japan. I detta sammanhang skulle Europeiska dataskyddsstyrelsen vilja bekräfta det tillvägagångssätt som redan antagits av dess föregångare när den skulle avge ett yttrande om skölden för skydd av privatlivet i EU och Förenta staterna. När artikel 29-arbetsgruppen avgav ett yttrande om skölden för skydd av privatlivet inkluderade den i sin analys Förenta staternas befogenheter och begränsningar att övervaka data ”på väg” till Förenta staterna[86]. Med tillämpning av samma standard för beslut om adekvat skydd i Japan anser Europeiska dataskyddsstyrelsen att information om de japanska myndigheternas befogenheter att övervaka uppgifter ”på väg” till Japan är relevanta. Om dessa övervakningsbefogenheter existerar tycks även Europadomstolens dom i målet Big Brother Watch tyda på att sådana befogenheter skulle behöva regleras i enlighet med de normer som Europadomstolen fastställt.

221. Mot denna bakgrund kan avlyssning som är begränsad till ”stöd till militära åtgärder” mycket väl sakna betydelse för bedömningen av beslutet om adekvat skyddsnivå. Europeiska dataskyddsstyrelsen önskar därför erhålla förtydliganden om de övervakningsåtgärder som japanska statliga enheter vidtar. I detta avseende skulle ett sådant klargörande vara välkommet för att avgöra om uppgifter som ska överföras enligt denna ram för en adekvat skyddsnivå skulle kunna bli föremål för tillgång för nationella säkerhetsändamål från de japanska behöriga myndigheterna inom detta område.

4.2.2 Frivilligt utlämnande av uppgifter i samband med nationell säkerhet

222. I förslaget till beslut om adekvat skyddsnivå anges att de fyra statliga organen endast har befogenhet att samla in (elektronisk) information genom frivilligt utlämnande av uppgifter. Enligt förslaget till beslut och bilaga II föreligger vissa lagstadgade begränsningar, vilket innebär att insamlingen av uppgifter begränsas till vad som är nödvändigt för att organen ska kunna utföra sina uppgifter.

223. Inom det straffrättsliga området, såsom anges i avsnittet om brottsbekämpning, är frivilligt utlämnande endast tillåtet som en del av en brottsutredning, och förutsätter således en konkret misstanke om att ett brott har begåtts. Undersökningar på området för nationell säkerhet skiljer sig från undersökningar på området för brottsbekämpning. Europeiska dataskyddsstyrelsen medger att de centrala principerna ”behov av utredning” och ”lämplig metod” enligt bilaga II är tillämpliga på ett liknande sätt inom området för nationell säkerhet och ska iakttas med vederbörlig hänsyn till de särskilda omständigheterna i varje enskilt fall[87]. Europeiska dataskyddsstyrelsen beklagar att

[86] Se WP255, EU-U.S. Privacy Shield –First annual joint review (ej översatt till svenska), antagen den 28 november 2017, s. 16: ”Artikel 29-arbetsgruppen anser att analysen av lagstiftningen i det tredjeland för vilket adekvat skyddsnivå övervägs inte bör begränsas till lagstiftning och praxis som möjliggör övervakning inom landets fysiska gränser, utan även bör omfatta en analys av de rättsliga grunderna i detta tredjelands lagstiftning som gör det möjligt för det att genomföra övervakning utanför sitt territorium när det gäller uppgifter från EU. Såsom redan framhållits i dess tidigare yttrande ”bör det stå klart att principerna för skölden för skydd av privatlivet ska tillämpas från och med den tidpunkt då överföringen av uppgifter äger rum, vilket innebär att uppgifter ”på väg” till det landet ska omfattas”.

[87] Se bilaga II s. 23.

tillämpningen inte har klargjorts ytterligare, t.ex. genom ytterligare hänvisningar till rättspraxis. Europeiska dataskyddsstyrelsen konstaterar dock att användningen av detta förfarande måste vara proportionerligt eller nödvändigt.

224. När personuppgifter har samlats in (”erhållits”) styrs hanteringen enligt förslaget till beslut av APPIHAO, med undantag för den regionala polisen[88]. I bilaga II anges att den regionala polisens hantering av personuppgifter regleras genom regionala föreskrifter som innehåller principer för skydd av personlig information, rättigheter och skyldigheter som är likvärdiga med dem i APPIHAO[89]. Eftersom det inte finns några tillgängliga engelska översättningar av dessa förordningar kan Europeiska dataskyddsstyrelsen inte bedöma om principerna är likvärdiga med principerna i APPIHAO.

225. Vad gäller ytterligare synpunkter avseende frivilligt utlämnande av uppgifter hänvisas till avsnittet om brottsbekämpning.

4.2.3 Tillsyn

4.2.3.1 Allmänna synpunkter

226. De fyra statliga organ som av nationella säkerhetsskäl har befogenhet att samla in elektronisk information som innehas av japanska företagare är följande: i) kansliet för information och forskning, ii) försvarsministeriet, iii) polisen (både den nationella polismyndigheten [90] och den regionala polisen) och iv) underrättelsetjänsten för allmän säkerhet.

227. Enligt förslaget till beslut om adekvat skyddsnivå är dessa statliga organ föremål för tillsyn från tre statliga organ på olika nivåer[91]. Europeiska dataskyddsstyrelsen noterar att det finns tillsynsmekanismer inom den lagstiftande delen (det japanska parlamentet) och den verkställande delen (generalinspektörens kansli för regelefterlevnad (nedan kallad *IGO*), de regionala kommissionerna för allmän säkerhet och kommissionen för granskning av den allmänna säkerheten). Europeiska dataskyddsstyrelsen betonar att kommissionen bör klargöra den rättsliga tillsynen (ex officio/garanti C i WP 237, för prövning föreligger ett särskilt kapitel i förslaget till beslut och en extra garanti i WP 237) för ovannämnda statliga organ, eftersom det är oklart om det finns en sådan rättslig tillsyn när det gäller insamling av personuppgifter för nationella säkerhetsändamål utan tvångsmedel.

4.2.3.2 Tillsyn från det japanska parlamentet

228. Europeiska dataskyddsstyrelsen noterar att det japanska parlamentet kan genomföra utredningar av offentliga myndigheters verksamhet, och därmed även för alla ovannämnda statliga enheter. Dessutom kan parlamentet begära framtagande av handlingar och vittnesuppgifter (artikel 62 i den japanska författningen, artikel 104 i lagen om parlamentet). Europeiska dataskyddsstyrelsen påpekar också att parlamentsledamöter enligt artiklarna 74 och 75 i lagen om parlamentet kan ställa skriftliga frågor till kansliet, vilka kan besvaras av kansliet (artikel 75 i lagen om parlamentet). Slutligen konstateras även att det finns särskilda rapporteringsskyldigheter för till exempel underrättelsetjänsten för allmän säkerhet (artikel 36 SAPA/artikel 31 ACO), genom en årlig rapport till parlamentet. Europeiska dataskyddsstyrelsen har inte erhållit någon sådan rapport.

[88] Beslut om adekvat skyddsnivå, punkterna 118 och 157.
[89] Se bilaga II s. 3.
[90] Enligt den erhållna informationen är emellertid den nationella polismyndighetens viktigaste uppgift att samordna utredningarna från de olika regionala polisavdelningarna, och dess insamling av information är begränsad till utbyten med utländska myndigheter.
[91] Se bilaga II s. 39.

4.2.3.3 Tillsyn från generalinspektören kansli för regelefterlevnad (IGO)

229. Europeiska dataskyddsstyrelsen noterar att det finns ett tillsynsorgan för försvarsministeriet som kallas IGO. Europeiska dataskyddsstyrelsen har inte erhållit lagen om inrättande av försvarsministeriet, utan enbart uppgifterna i bilaga II till förslaget till beslut. Enligt bilaga II är IGO ett oberoende kansli inom försvarsministeriet, som står under direkt tillsyn från försvarsministern i enlighet med artikel 29 i lagen om inrättandet av försvarsministeriet. IGO har befogenhet att utföra inspektioner av efterlevnaden av lagar och andra författningar från försvarsministeriets tjänstemän (så kallade ”försvarsinspektioner”), inom hela ministeriet, inbegripet självförsvarsstyrkorna.

230. Enligt bilaga II ska IGO utföra sina uppgifter oberoende av försvarsministeriets operativa avdelningar. Europeiska dataskyddsstyrelsen noterar att IGO är ett *internt* tillsynsorgan.

231. Inspektionerna leder fram till bedömningar och, i syfte att säkerställa efterlevnad, åtgärder som rapporteras direkt till försvarsministern. På grundval av IGO:s rapport kan försvarsministern utfärda föreläggganden för att genomföra de åtgärder som krävs för att komma till rätta med situationen. Vice försvarsministern är ansvarig för genomförandet av dessa åtgärder och ska rapportera till försvarsministern om statusen för ett sådant genomförande.

232. Europeiska dataskyddsstyrelsen har analyserat bilaga II, utan att ha erhållit de rättsliga bestämmelserna (lagen om inrättandet av försvarsministeriet) och välkomnar möjligheten att begära nödvändiga åtgärder för att rätta till situationen. Europeiska dataskyddsstyrelsen ifrågasätter dock IGO:s oberoende, eftersom det är frågan om ett kansli inom försvarsministeriet och står under försvarsministerns direkta tillsyn i enlighet med bilaga II (enligt WP 237 ”är det inte i sig tillräckligt med funktionell självständighet för att skydda denna tillsynsmyndighet från all extern påverkan”).

233. I överensstämmelse med rättspraxis från Europadomstolen och WP 237 och i enlighet med vad som anges i bilaga II kan generalinspektören begära rapporter från det berörda kansliet (dokument, webbplatser, förklaringar). Europeiska dataskyddsstyrelsen anser att det krävs förtydliganden huruvida de berörda kontoren är skyldiga att följa dessa krav eller inte och om de begärda handlingarna omfattar sekretessbelagt material, såsom det som anges i WP 237.

234. Även om Europeiska dataskyddsstyrelsen välkomnar att juridiska experter i mycket högt uppsatta poster (tidigare chefsåklagare) leder IGO, förefaller det nödvändigt att klargöra formerna för utnämningen till detta tillsynsorgan.

4.2.3.4 Tillsyn från kommissionen för granskning av den allmänna säkerheten

235. Enligt bilaga II (sidan 25) ska underrättelsetjänsten för allmän säkerhet genomföra regelbundna och särskilda kontroller av verksamheten vid sina enskilda byråer och kanslier (byrån för allmän säkerhet och underrättelseverksamhet, kanslier för allmän säkerhet och underrättelseverksamhet och underordnade kanslier etc.). För den regelbundna inspektionen utses en biträdande generaldirektör och/eller en direktör som inspektörer. Sådana inspektioner bör också omfatta hanteringen av personuppgifter.

236. Enligt skäl 163 i förslaget till beslut fungerar kommissionen för granskning av den allmänna säkerheten som ett oberoende organ för förhandskontroll av underrättelsetjänsten för allmän säkerhet, med avseende på ACO[92] och SAPA[93]. Europeiska dataskyddsstyrelsen välkomnar detta.

[92] Lag om kontroll av organisationer som har begått urskillningslösa massmord (lag nr 147 av den 7 december 1999).
[93] Lagen om förebyggande åtgärder (lag nr 240 av den 21 juli 1952).

237. Även om det japanska justitieministeriets webbplats ger viss information[94], är Europeiska dataskyddsstyrelsen inte i stånd att göra en noggrann bedömning av huruvida kommissionen för granskning av den allmänna säkerheten är oberoende, eftersom den inte har erhållit lagen om inrättande av kommissionen för granskning av den allmänna säkerheten[95] och reglerna för kommissionen för granskning av den allmänna säkerheten[96].

4.2.3.5 Tillsyn från den nationella kommissionen för allmän säkerhet, de regionala kommissionerna för allmän säkerhet och APPIHAO (verkställande)

238. Se 3.1.2.2.1 (nationella kommissionen för allmän säkerhet), 3.1.2.2.2. (de regionala kommissionerna för allmän säkerhet) och 3.1.2.2.4. (verkställighet).

4.2.3.6 Tillsyn från PPC

239. Europeiska dataskyddsstyrelsen uppmanar kommissionen att antingen ange i skäl 164 att PPC inte är ett tillsynsorgan för ovannämnda statliga organ och att myndigheten endast är behörig vid prövning för enskilda eller att flytta avsnittet i skäl 164 om PPC till avsnittet ”prövning för enskilda”.

4.2.4 Prövningsmekanism

240. Vid analysen av den prövningsmekanism som nyligen förhandlats fram hänvisas till avsnittet om brottsbekämpning.

241. Det är dessutom värt att notera att det enligt japansk lagstiftning föreskrivs en särskild möjlighet till individuell prövning inom området för nationell säkerhet. Europeiska dataskyddsstyrelsen är medveten om att alla enskilda personer, även enskilda personer i EU, i allmänhet kan begära att uppgifter lämnas ut, korrigeras (inklusive raderas) eller att förvaltningsorganens användning avbryts, även om uppgifterna behandlas för ändamål som rör nationell säkerhet. Om en sådan begäran ”avvisas på grund av att den berörda informationen inte anses kunna lämnas ut”, kan en förnyad prövning begäras och ”översynsnämnden för utlämning av uppgifter och skydd för personuppgifter” måste rådfrågas. Denna nämnd består av ledamöter som utses av premiärministern med samtycke från båda kamrarna, vilken har utredande befogenheter, och avslutar ärendet med en skriftlig rapport för den berörda enskilda personen, vilken inte är rättsligt bindande, men nästan alltid följs[97]. Enligt bilaga II hade en förvaltningsmyndighet endast i två fall av 2000 fattat ett beslut som inte överensstämde med nämndens slutsats.[98]

---

[94] Se http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (september 2018): Det utomministeriella organet ”består av en ordförande och sex ledamöter. *De väljs bland personer med god karaktär som kan göra en rättvis bedömning av organisationernas kontroll och har omfattande kunskaper och erfarenhet av både lagstiftning och samhälle. De utses av premiärministern och måste godkännas av båda kamrarna i parlamentet. När det gäller tillämpningen av de tidigare nämnda lagarna (SAPA/ACO) utför ledamöterna sina uppgifter helt oberoende, utan instruktioner eller övervakning från premiärministern eller justitieministern.”*

[95] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (september 2018).

[96] Artikel 28 ACO.

[97] Bilaga II, s. 25 och 26. Lagen om inrättande av översynsnämnden för utlämning av uppgifter och skydd för personuppgifter, artiklarna 4, 9 och 11.

[98] Bilaga II, fotnot 35.

242. Det förefaller följa av den förklaring som tillhandahållits att översynen inte är tillgänglig om informationen kan ”lämnas ut”, men den enskilda är missnöjd med resultatet. Europeiska dataskyddsstyrelsen erkänner denna möjlighet att överklaga, men önskar ytterligare klargöranden vad gäller sistnämnda aspekt, vilken avsevärt skulle begränsa dess räckvidd.

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)