Yttrande 32/2021 om Europeiska kommissionens förslag till genomförandebeslut enligt förordning (EU) 2016/679 om adekvat skydd av personuppgifter i Republiken Korea

Version 1.0

Antaget den 24 september 2021

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

INNEHÅLL

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 (nedan kallat *GDPR*),

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[1],

med beaktande av artiklarna 12 och 22 i arbetsordningen.

HÄRIGENOM FRAMFÖRS FÖLJANDE:

1. SAMMANFATTNING

1. Kommissionen lanserade den formella processen för att anta dess förslag till genomförandebeslut (nedan kallat *förslaget till beslut*) om adekvat skydd av personuppgifter i Republiken Korea enligt Personal Information Protection Act enligt GDPR den 16 juni 2021[2].

2. Samma dag begärde Europeiska kommissionen ett yttrande från Europeiska dataskyddsstyrelsen (nedan kallat *dataskyddsstyrelsen*)[3]. Europeiska dataskyddsstyrelsens bedömning av huruvida en adekvat skyddsnivå upprätthålls i Republiken Korea har gjorts på grundval av en granskning av själva förslaget till beslut samt utifrån en analys av den dokumentation som tillgängliggjorts[4] av kommissionen.

3. Vid sin bedömning har dataskyddsstyrelsen fokuserat både på de allmänna GDPR-aspekterna i förslaget till beslut och de offentliga myndigheternas tillgång till personuppgifter som överförts från EES för ändamål som hänför sig till brottsbekämpning och nationell säkerhet, inbegripet de rättsmedel som är tillgängliga för enskilda personer i EES. Dataskyddsstyrelsen har även bedömt om de skyddsåtgärder som föreskrivs enligt den sydkoreanska rättsliga ramen är införda och verkningsfulla.

4. Som sin främsta referens för detta arbete har dataskyddsstyrelsen använt GDPR:s referensram för adekvat skyddsnivå[5] (nedan kallat *GDPR:s referensram för adekvat skyddsnivå*) som antogs i februari 2018 samt dataskyddsstyrelsens Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder[6].

1.1. Konvergensområden

5. Dataskyddsstyrelsens huvudmål är att avge ett yttrande till kommissionen om huruvida en adekvat skyddsnivå tilldelas enskilda personer vars personuppgifter överförs till Republiken Korea. Det är

[1] Hänvisningar till ”medlemsstater” som görs i hela detta yttrande ska förstås som hänvisningar till ”EES-medlemsstater”.
[2] Se pressmeddelande https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Se föregående fotnot.
[4] Dataskyddsstyrelsen baserade sin analys på officiella översättningar som framställts av Sydkoreas regering.
[5] WP254, GDPR Adequacy Referential, den 6 februari 2018, (godkänd av dataskyddsstyrelsen, se https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Se dataskyddsstyrelsens Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder, antagen den 10 november 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

viktigt att veta att dataskyddsstyrelsen inte förväntar sig att den sydkoreanska ramen för uppgiftsskydd ska kopiera EU:s dataskyddslagstiftning.

6. För att en adekvat skyddsnivå ska anses föreligga erinrar dock dataskyddsstyrelsen om att tredjelandets lagstiftning, enligt artikel 45 i GDPR samt rättspraxis vid Europeiska unionens domstol (nedan kallat *EU-domstolen*), måste anpassas till det väsentliga innehållet i de grundläggande principer som fastställs i GDPR. I detta sammanhang uppvisar den sydkoreanska ramen för uppgiftsskydd många likheter med EU:s ram för uppgiftsskydd genom att ha en enda lagstiftningsakt som både täcker den offentliga och privata sektorn, och som färdigställs av sektorsspecifika lagstiftningsakter.

7. Vad gäller innehållet noterar dataskyddsstyrelsen viktiga områden som överensstämmer mellan GDPR-ramen och den sydkoreanska ramen för uppgiftsskydd vad gäller vissa centrala bestämmelser, såsom begrepp (t.ex. "personuppgifter", "behandling", "registrerad"); grunder för laglig och rättvis behandling för berättigade ändamål; ändamålsbegränsning; uppgifternas kvalitet och proportionalitet; lagring av uppgifter, säkerhet och konfidentialitet; öppenhet; samt särskilda kategorier av uppgifter.

8. Förutom detta välkomnar dataskyddsstyrelsen de ansträngningar som kommissionen och de sydkoreanska myndigheterna gjort för att säkerställa tillhandahållandet av en adekvat skyddsnivå i Republiken Korea i linje med den i GDPR genom att den sydkoreanska tillsynsmyndigheten antar meddelanden (som inte bara gäller för personuppgifter som överförs från EES till Sydkorea) för att fylla i luckorna mellan GDPR och den sydkoreanska ramen för uppgiftsskydd. I detta sammanhang vill dataskyddsstyrelsen lyfta fram relevansen av dessa meddelanden för bedömningen av en adekvat skyddsnivå i Republiken Korea, och noterar att de t.ex. innehåller relevanta förtydliganden om vissa viktiga skyddsåtgärder, bland annat i förhållande till tillämpningsområdet för undantagen från PIPA för behandlingen av pseudonymiserade personuppgifter för ändamål som hänför sig till vetenskap, forskning och statistik, vidare överföringar samt de tillämpliga reglerna i samband med offentliga myndigheters tillgång till uppgifter.

1.2. Utmaningar

9. Samtidigt som dataskyddsstyrelsen har identifierat många aspekter av den sydkoreanska ramen för uppgiftsskydd som väsentligen likvärdiga med EU:s ram för uppgiftsskydd, finner den även att vissa aspekter kan behöva närmare undersökas och förtydligas. Dataskyddsstyrelsen finner särskilt att följande poster bör närmare bedömas för att säkerställa att den väsentligen likvärdiga skyddsnivån uppfylls, och att de bör noggrant övervakas av Europeiska kommissionen.

1.2.1. Allmänt

10. Dataskyddsstyrelsen noterar att meddelande nr 2021-1 *fungerar som en administrativ regel med rättsligt bindande verkan på den personuppgiftsansvarige såtillvida att all överträdelse av meddelandet kan betraktas om en överträdelse av de relevanta bestämmelserna i PIPA*[7]. Meddelandet innehåller inga ytterligare regler i sig, utan snarare förtydliganden om hur lagtexten till PIPA ska förstås för att gälla. Mot bakgrund av dess övergripande betydelse vad gäller PIPA:s bestämmelser om pseudonymisering, som dataskyddsstyrelsen förstår är föremål för pågående rättsfall, uppmanar dataskyddsstyrelsen därför kommissionen att lämna närmare information om den bindande karaktären, verkställbarheten och giltigheten av meddelande nr 2021-1, och rekommenderar att dess praktiska efterlevnad noga kontrolleras, särskilt dess tillämpning av den sydkoreanska tillsynsmyndigheten men också av domstolar, särskilt när den motsvarande skyddsnivån som ges av den sydkoreanska rättsliga ramen baseras på de förtydliganden som ges däri.

[7] Se avsnitt I i bilaga I till förslaget till beslut.

1.2.2. Allmänna dataskyddsaspekter

11. Vad gäller tillämpningsområdet för beslutet om adekvat skyddsnivå noterar dataskyddsstyrelsen att det kommer att omfatta överföringar från EES:s rättsliga ram till både offentliga och privata "personuppgiftsansvariga" som omfattas av PIPA:s tillämpningsområde. Dataskyddsstyrelsen förstår att enheter som enligt GDPR fungerar som personuppgiftsbiträden ingår i denna term. För att undvika missförstånd uppmanar dock dataskyddsstyrelsen kommissionen att förtydliga att beslutet om adekvat skyddsnivå också kommer att innefatta överföringar till "personuppgiftsbiträden" i Sydkorea.

12. En viktig aspekt som dataskyddsstyrelsen vill uppmärksamma gäller begreppet pseudonymiserade uppgifter i den sydkoreanska ramen för uppgiftsskydd. Enligt sydkoreansk lagstiftning omfattas behandling av pseudonymiserade personuppgifter av undantag från ett antal relevanta bestämmelser, däribland bestämmelserna för enskilda registrerades rättigheter samt lagring av uppgifter. Enligt Europeiska kommissionen sker detta bara när pseudonymiserade personuppgifter behandlas för ändamål som hänför sig till statistik, vetenskaplig forskning eller arkivering i det allmännas intresse. Detta påstående styrks dock främst av meddelande nr 2021-1, vilket gör det redan nämnda behovet av ytterligare information om meddelandets bindande karaktär, verkställbarhet och giltighet, samt övervakningen av detta, i sammanhanget högst relevanta, meddelande. Dataskyddsstyrelsen uppmanar även kommissionen att närmare bedöma effekten av pseudonymisering enligt sydkoreansk lagstiftning och – allra viktigast – hur den kan påverka de grundläggande rättigheterna och friheterna för de registrerade vars personuppgifter överförs till Republiken Korea enligt beslutet om adekvat skyddsnivå. Dataskyddsstyrelsen uppmanar i synnerhet kommission att närmare bedöma undantagen i artikel 28.7 i PIPA och artikel 40.3 i CIA samt att noga övervaka deras tillämpning och relevant rättspraxis för att säkerställa att de registrerades rättigheter inte orimligen begränsas när personuppgifter som överförs enligt beslutet om adekvat skyddsnivå behandlas för dessa syften.

13. Vidare noterar dataskyddsstyrelsen att sydkoreansk lagstiftning medger en rätt att återkalla sitt samtycke endast under specifika omständigheter och uppmanar därför kommissionen att närmare bedöma effekten av en brist på en allmän rätt att återkalla sitt samtycke, och att lämna ytterligare försäkringar för att tillse att en väsentlig nivå av uppgiftsskydd alltid garanteras, också genom att vid behov förtydliga den roll som intas av rätten till upphävande enligt PIPA i frånvaro av en allmän rätt att återkalla sitt samtycke.

14. Vad gäller vidare överföringar erkänner dataskyddsstyrelsen att den registrerades informerade samtycke i allmänhet kommer att användas som grund för uppgiftsöverföringar från en personuppgiftsansvarig baserad i Sydkorea till en tredjelandsbaserad mottagare och att det i meddelande nr 2021-1 anges att enskilda personer måste informeras om det tredjeland till vilket deras uppgifter kommer att överföras. Dataskyddsstyrelsen uppmanar dock kommissionen att säkerställa att den information som den registrerade ska få också innehåller information om de möjliga riskerna med överföringar till följd av avsaknaden av adekvat skydd i tredjelandet liksom avsaknaden av lämpliga skyddsåtgärder. Vidare välkomnar dataskyddsstyrelsen garantier i beslutet om adekvat skyddsnivå om att personuppgifter inte kommer att överföras från sydkoreanska personuppgiftsansvariga till ett tredjeland i någon situation där ett giltigt samtycke enligt GDPR inte kan lämnas, t.ex. på grund av en obalans i befogenheter.

15. Vad gäller utnämningen av ledamöterna i den sydkoreanska tillsynsmyndigheten uppmanar dataskyddsstyrelsen kommissionen att övervaka all utveckling som skulle kunna påverka ledamöternas oberoende i den sydkoreanska tillsynsmyndigheten, även om det formella förfarandet skulle överensstämma med GDPR och därför uppfylla kravet på likvärdighet med EES:s rättsliga ram.

16. Vad gäller budgeten – återigen baserat på den information som lämnas av Europeiska kommissionen – görs ingen hänvisning till enskildheterna hos den personal som utses till PIPC eller till de anslag som

ställts till dess förfogande. Dataskyddsstyrelsen välkomnar därför ytterligare information i förslaget till beslut om dessa två relevanta ämnen.

1.2.3. Om offentliga myndigheters tillgång till uppgifter som överförts till Republiken Korea

17. Dataskyddsstyrelsen har även analyserat den sydkoreanska rättsliga ramen avseende statlig tillgång för ändamål som hänför sig till brottsbekämpning och nationell säkerhet till personuppgifter som överförs från EES till Sydkorea. Samtidigt som dataskyddsstyrelsen är medveten om utfästelserna och försäkringarna från Sydkoreas regering, enligt bilaga II till förslaget till beslut, har den identifierat ett antal aspekter som måste förtydligas eller väcker farhågor.

18. Dataskyddsstyrelsen noterar att PIPA:s bestämmelser är tillämpliga utan begränsning på området för brottsbekämpning. Dataskyddsstyrelsen noterar även att behandlingen av personuppgifter på området nationell säkerhet är underkastad en mer begränsad uppsättning bestämmelser i PIPA.

19. Vad gäller det frivilliga utlämnandet av personuppgifter från teleoperatörer till nationella säkerhetsmyndigheter befarar dataskyddsstyrelsen att förhållandet mellan avsnitt 3 i bilaga I till förslaget till beslut, där det anges att operatörer i princip måste meddela berörda enskilda personer när de frivilligt tillmötesgår en begäran, och artikel 58.1. 2 i PIPA, dvs. det delvisa undantaget för ändamål som hänför sig till nationell säkerhet, är oklart. Detta kan göra informationskraven ineffektiva, så att de registrerade får det avsevärt svårare att hävda sin rätt till uppgiftsskydd, särskilt avseende rättsmedel.

20. Även om det inte uttryckligen anges i förslaget till beslut, förstår dataskyddsstyrelsen av kommissionens förklaringar att den sydkoreanska rättsliga ramen inte medger massavlyssning av telekommunikationsuppgifter. Därför skulle aktuell rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna om förfaranden för massavlyssning inte vara direkt relevant för bedömningen av nivån av uppgiftsskydd i Sydkorea.

21. Förslaget till beslut innehåller ingen information om den rättsliga ramen för vidare överföringar på området för nationell säkerhet. Dataskyddsstyrelsen förstår att vidare överföringar för ändamål som hänför sig till nationell säkerhet enligt kommissionens mening är tillräckligt reglerade genom de allmänna skyddsåtgärderna och principerna i den konstitutionella ramen och PIPA, men hyser farhågor över huruvida detta kan anses uppfylla kraven på precision och klarhet i lagen och fastställer verkningsfulla och verkställbara skyddsåtgärder. De skyddsåtgärder som kommissionen hänvisar till är mycket allmänt hållna och behandlar inte, på rättslig grund, de specifika omständigheter och villkor under vilka vidare överföringar för ändamål som hänför sig till nationell säkerhet kan ske. I detta sammanhang noterar dataskyddsstyrelsen även att kommissionen inte har beaktat förekomsten av internationella avtal som har slutits mellan Republiken Korea och tredjeländer eller internationella organisationer, i vilka särskilda bestämmelser kan vara föreskrivna för internationell överföring av personuppgifter av brottsbekämpande myndigheter och/eller underrättelsetjänster till tredjeländer. Dataskyddsstyrelsen finner att slutandet av bilaterala eller multilaterala avtal med tredjeländer för ändamål som hänför sig till brottsbekämpnings- eller underrättelsesamarbete sannolikt påverkar den sydkoreanska ramen för uppgiftsskydd enligt bedömning.

22. Dataskyddsstyrelsen noterar att tillsynen över genomförandet av strafflagstiftningen liksom nationella säkerhetsmyndigheter garanteras av en kombination av olika interna och externa organ, i synnerhet PIPC, som är försedd med tillräckliga genomförandebefogenheter.

23. För att rättsmedel och prövningar ska vara effektiva måste de registrerade kunna vända sig till ett behörigt organ som uppfyller kraven i artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallat *stadgan*), dvs. som är behörigt att avgöra att en uppgiftsbehandling föreligger, liksom kontrollera behandlingens laglighet, och som har effektiva korrigerande befogenheter ifall uppgiftsbehandlingen är olaglig. Dataskyddsstyrelsen ber därför kommissionen att

klargöra om ett klagomål till PIPC eller någon annan talan inför en domstol underkastas krav i sak och/eller förfarandemässiga krav, såsom en bevisbörda, och om enskilda personer i EES skulle kunna uppfylla ett sådant förhandsvillkor.

1.3. Slutsats

24. Dataskyddsstyrelsen finner att beslutet om adekvat skyddsnivå är av stor betydelse, också med hänsyn tagen till att det – med de undantag som betonas i yttrandet – kommer att omfatta överföringar både i den offentliga och privata sektorn.

25. Dataskyddsstyrelsen välkomnar de ansträngningar som gjorts av kommissionen och de sydkoreanska myndigheterna för att anpassa den sydkoreanska rättsliga ramen till EU:s rättsliga ram. De förbättringar som är inplanerade genom meddelande nr 2021-1 för att överbrygga några av skillnaderna mellan de två ramarna är mycket viktiga och tas väl emot. Dataskyddsstyrelsen noterar dock att ett antal farhågor kvarstår, även vad gäller meddelande nr 2021-1, som är kopplade till nödvändigheten att närmare klargöra andra frågor, och rekommenderar därför kommissionen att ta upp de farhågor och framställningar om förtydligande som väckts av dataskyddsstyrelsen och att lämna ytterligare information och förklaringar till de frågor som väckts i detta yttrande.

2. INLEDNING

2.1. Den sydkoreanska ramen för uppgiftsskydd

26. Den huvudsakliga lagstiftningsakt som reglerar uppgiftsskyddet i Republiken Korea är Personal Information Protection Act (lag nr 10465 av den 29 mars 2011, senast ändrad genom lag nr 16930 av den 4 februari 2020, nedan kallat *PIPA*). Den kompletteras av en genomförandeförordning (presidentdekret nr 23169 av den 29 september 2011, senast ändrad genom presidentdekret nr 30892 av den 4 augusti 2020, nedan kallat *PIPA:s genomförandeförordning*), som är rättsligt bindande och verkställbar.

27. Utöver PIPA innefattar den sydkoreanska ramen för uppgiftsskydd föreskrivande ”meddelanden” som ges ut av den sydkoreanska tillsynsmyndigheten, Personal Information Protection Commission (nedan kallat *PIPC*), som tillhandahåller ytterligare regler om tolkningen och tillämpningen av PIPA. Nyligen antog PIPC meddelande nr 2021-1 av den 21 januari 2021 (som ändrade det tidigare meddelandet nr 2020-10 av den 1 september 2020, nedan kallat *meddelande nr 2020-10*) om tolkningen, tillämpningen och genomförandet av vissa bestämmelser i PIPA. Mer specifikt var detta meddelande resultatet av diskussioner mellan sydkoreanska myndigheter och kommissionen om en adekvat skyddsnivå. Det innehåller förtydliganden om tillämpningen av specifika bestämmelser i PIPA, inräknat behandlingen av personuppgifter som överförs till Sydkorea på grundval av det planerade beslutet om adekvat skyddsnivå[8] och det fungerar som en administrativ regel med rättsligt bindande verkan på den personuppgiftsansvarige såtillvida att all överträdelse av meddelandet kan betraktas om en överträdelse av de relevanta bestämmelserna i PIPA[9]. I detta sammanhang vill dataskyddsstyrelsen notera att meddelandet visserligen omnämns som ”tilläggsregler” i förslaget till beslut men inte innefattar några ytterligare regler i sig, utan snarare förklaringar som ska förtydliga hur lagtexten till PIPA ska förstås att gälla, särskilt vad gäller personuppgifter som överförts från EES. Dataskyddsstyrelsen rekommenderar därför att den praktiska efterlevnaden av meddelande nr 2021-1 noga kontrolleras, särskilt dess tillämpning, men inte bara av PIPC utan också av domstolar, i synnerhet när den motsvarande skyddsnivå som ges av den sydkoreanska rättsliga ramen baseras på de förtydliganden som ges i meddelande nr 2021-1.

[8] Se avsnitt I i bilaga I till förslaget till beslut.
[9] Se föregående fotnot.

28. I andra relevanta dataskyddslagar i den sydkoreanska rättsliga ramen fastställs regler om behandlingen av personuppgifter i specifika industrisektorer såsom:

- Lagen Act on the Use and Protection of Credit Information (nedan kallat *CIA*), med dess genomförandeförordning (nedan kallat *CIA:s genomförandeförordning*), innehåller specifika regler för kommersiella operatörer och specialiserade enheter (t.ex. kreditvärderingsinstitut, finansinstitut) när de behandlar personliga kreditupplysningar som behövs för att avgöra kreditvärdigheten för parter till finansiella eller kommersiella transaktioner.
- Lagen Act on the Promotion of Information and Communications Network Utilisation and Data Protection (nedan kallat *nätverkslagen*).
- Lagen Communications Privacy Protection Act (nedan kallat *CCPA*).

29. På området statlig tillgång, utöver de relevanta bestämmelserna i PIPA och CPPA, har dataskyddsstyrelsen även övervägt vissa andra lagstiftningsakter, dvs. Criminal Procedure Act (nedan kallat *CPA*), Telecommunications Business Act (nedan kallat *TBA)*, Act on Reporting and Using Specified Financial Transaction Information (nedan kallat *ARUSFTI*) samt National Intelligence Service Act (nedan kallat *NISA*).

2.2. Omfattningen av Europeiska dataskyddsstyrelsens bedömning

30. Europeiska kommissionens förslag till beslut är resultatet av en bedömning av den sydkoreanska ramen för uppgiftsskydd, vilken följts av diskussioner med den sydkoreanska regeringen. Enligt artikel 70.1 s i GDPR förväntas Europeiska dataskyddsstyrelsen avge ett oberoende yttrande om kommissionens bedömningar, identifiera eventuella brister i den rättsliga ramen för adekvat skyddsnivå, och sträva efter att lägga fram förslag om hur dessa ska åtgärdas.

31. För att undvika upprepningar och i avsikt att bidra till bedömningen av den sydkoreanska rättsliga ramen har dataskyddsstyrelsen valt att fokusera på vissa specifika punkter i förslaget till beslut samt att överlämna sin analys och sitt yttrande om dem, och avstå från att återge de flesta av de faktiska omständigheter och bedömningar där dataskyddsstyrelsen inte har någon anledning att anta att lagstiftningen i Republiken Korea inte skulle vara väsentligen likvärdig med lagstiftningen i EES. I linje med EU-domstolens rättspraxis täcker en mycket stor del av analysen dessutom den rättsliga ordningen för tillgång till personuppgifter som överförs till Republiken Korea avseende nationell säkerhet, samt praxis vid dess nationella säkerhetsapparat.

32. I sin bedömning har dataskyddsstyrelsen beaktat EU:s tillämpliga ram för uppgiftsskydd, inräknat artiklarna 7, 8 och 47 i stadgan, respektive skyddet av rätten till privat- och familjeliv, rätten till skydd av personuppgifter och rätten till ett effektivt rättsmedel och en opartisk domstol, samt artikel 8 i Europakonventionen om skyddet av rätten till privat- och familjeliv. Utöver detta har Europeiska dataskyddsstyrelsen beaktat kraven i GDPR samt relevant rättspraxis.

33. Syftet med denna åtgärd är att förse kommissionen med ett yttrande om bedömningen av huruvida en adekvat skyddsnivå upprätthålls i Republiken Korea. Begreppet ”adekvat skyddsnivå”, som redan ingick i direktiv 95/46, har vidareutvecklats av EU-domstolen. Det är viktigt att erinra om den standard som fastställts av EU-domstolen i domen i målet Schrems I, nämligen att ”skyddsnivån” i tredjelandet 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]”[10]. 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. En adekvat

[10] C-362/14, *Maximilian Schrems mot Data Protection Commissioner*, den 6 oktober 2015, ECLI:EU:C:2015:650, punkterna 73–74.

skyddsnivå kan uppnås genom en kombination av rättigheter för de registrerade och skyldigheter för dem som behandlar personuppgifter, eller som utövar kontroll över en sådan behandling och tillsyn av oberoende organ. Reglerna om uppgiftsskydd är dock bara verkningsfulla 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 om uppgiftsskydd ska vara effektiva[11].

2.3. Allmänna synpunkter och farhågor

2.3.1. Internationella åtaganden som ingåtts av Republiken Korea

34. I enlighet med artikel 45.2 c i GDPR och GDPR:s referensram för adekvat skyddsnivå[12] 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 avseende skyddet av personuppgifter, samt genomförandet av sådana skyldigheter.

35. Sydkorea är part i flera internationella avtal som garanterar rätten till personlig integritet, t.ex. den internationella konventionen om medborgerliga och politiska rättigheter (artikel 17), konventionen om rättigheter för personer med funktionsnedsättning (artikel 22) samt barnkonventionen (artikel 16). Som medlem i OECD ställer sig Sydkorea dessutom bakom OECD:s ram för integritetsskydd, särskilt riktlinjerna för integritetsskydd och gränsöverskridande flöden av personuppgifter.

36. Dataskyddsstyrelsen noterar även Sydkoreas medverkan som observatörsstat i arbetet inom den rådgivande kommittén till Europarådets konvention 108+, även om landet ännu inte har beslutat om det ska ansluta sig.

2.3.2. Tillämpningsområdet för beslutet om adekvat skyddsnivå

37. Enligt skäl 5 i förslaget till beslut finner kommissionen att Republiken Korea säkerställer en adekvat skyddsnivå för personuppgifter som överförs från en personuppgiftsansvarig eller ett personuppgiftsbiträde i EU till personuppgiftsansvariga (t.ex. fysiska eller juridiska personer, organisationer, offentliga institutioner) som omfattas av PIPA:s tillämpningsområde, med undantag för religiösa organisationers behandling av personuppgifter för missionsverksamhet och politiska partiers nominering av kandidater[13], eller behandlingen av personliga kreditupplysningar enligt CIA av personuppgiftsansvariga som står under tillsyn av kommissionen för finansiella tjänster.

38. Dataskyddsstyrelsen noterar att beslutet om adekvat skyddsnivå kommer att omfatta överföringar från EES:s rättsliga ram till både offentliga och privata "personuppgiftsansvariga" som omfattas av PIPA:s tillämpningsområde. Dataskyddsstyrelsen förstår att termen "personuppgiftsansvariga" också omfattar enheter som enligt GDPR fungerar som personuppgiftsbiträden, med tanke på att PIPA kommer att gälla för dem i samma omfattning och att särskilda skyldigheter gäller när en personuppgiftsansvarig (den "som lägger ut på entreprenad") anlitar en tredje part för behandlingen av personuppgifter ("entreprenören"). För att undvika missförstånd uppmanar dock dataskyddsstyrelsen kommissionen att förtydliga att beslutet om adekvat skyddsnivå också kommer att omfatta överföringar till "personuppgiftsbiträden" i Sydkorea och att skyddsnivån för personuppgifter som överförs från EES inte heller i dessa fall kommer att undergrävas.

[11] WP254, s.2.
[12] WP254, s.2.
[13] För närmare beskrivning, se nedan i avsnitt 3.1.2 i detta yttrande.

39. Med tanke på att beslutet om adekvat skyddsnivå också innefattar överföringar av personuppgifter mellan offentliga organ, förstår dataskyddsstyrelsen att detta även kommer att täcka överföringar mellan tillsynsmyndigheter för uppgiftsskydd, och uppmanar för tydlighetens skull kommissionen att också åtgärda denna fråga.

40. Vad gäller de enheter som undantagits från tillämpningsområdet för beslutet om adekvat skyddsnivå vill dataskyddsstyrelsen vidare betona att beslutet om adekvat skyddsnivå kan gynnas av en tydligare identifiering av de ”kommersiella organisationer” som står under tillsyn av PIPC (artikel 45.3 i CIA), så att EES-baserade personuppgiftsansvariga och personuppgiftsbiträden lätt kan bedöma om importören också omfattas av tillämpningsområdet för beslutet om adekvat skyddsnivå innan uppgifter överförs till enheter som omfattas av tillämpningsområdet för CIA eller, åtminstone, varnas om nödvändigheten att bedöma denna aspekt.

41. Vad gäller tillämpningsområdet för beslutet om adekvat skyddsnivå förstod dataskyddsstyrelsen av kommissionens närmare förklaringar att Sydkoreas finansunderrättelseenhet (nedan kallat *KOFIU*), som är inrättad enligt kommissionen för finansiella tjänster och övervakar förebyggandet av penningtvätt och finansiering av terrorism enligt ARUSFTI[14], också har undantagits från tillämpningsområdet, då den endast har domsrätt över finansinstitut som inte själva ingår i förslaget till beslut. Artikel 1.2 c i förslaget till beslut undantar dock från sitt tillämpningsområde endast de personuppgiftsansvariga som står under tillsyn av kommissionen för finansiella tjänster och behandlar personliga kreditupplysningar enligt CIA. Mot denna bakgrund ber dataskyddsstyrelsen kommissionen att klargöra huruvida KOFIU och de uppgiftsbehandlingar som utförs av KOFIU själv omfattas av förslaget till beslut.

3. ALLMÄNNA DATASKYDDSASPEKTER

3.1. Innehållsmässiga principer

42. I kapitel 3 i GDPR:s referensram för adekvat skyddsnivå behandlas de innehållsmässiga principerna. Ett tredjelands system måste innehålla dessa för att den tillhandahållna skyddsnivån ska anses väsentligen likvärdig med den skyddsnivå som garanteras genom EU-lagstiftningen.

43. Även om rätten till skydd av personuppgifter inte är uttryckligen inskriven i den sydkoreanska författningen i sig, erkänns den som en grundläggande rättighet i de grundlagsfästa rättigheterna till mänsklig värdighet och eftersträvandet av lycka (artikel 10), privatliv (artikel 17) och personlig integritet i kommunikationstjänster (artikel 18). Detta har bekräftats av både Högsta domstolen och författningsdomstolen, enligt hänvisning i kommissionens förslag till beslut[15]. Dataskyddsstyrelsen noterar detta erkännande då den därav drar slutsatsen att uppgiftsskydd som grundläggande rättighet, enligt artikel 37 i den sydkoreanska författningen, ”endast får begränsas enligt lag och när det är nödvändigt för den nationella säkerheten, eller upprätthållandet av lag och ordning eller för den allmänna välfärden” och att ”sådana begränsningar, också när de införs, inte får påverka rättighetens eller frihetens väsentliga innehåll”.

44. Enligt Europeiska kommissionen[16] har författningsdomstolen fastställt att också utlänningar omfattas av grundläggande rättigheter. Även om rättspraxis hittills inte specifikt hanterat icke-koreanska medborgares rätt till personlig integritet, är det, enligt de officiella representationerna från den sydkoreanska regeringen[17], allmänt accepterat bland forskare att ”människors rättigheter” är fastställda i artiklarna 12–22 i författningen. Vidare har Republiken Korea antagit flera lagar på

[14] Se bilaga II, avsnitt 2.2.3.1.
[15] Se skäl 8 i förslaget till beslut och relevant rättspraxis som omnämns i fotnot 10 till förslaget till beslut, för vilken bara sammanfattningar på engelska finns att tillgå.
[16] Se skäl 9 i förslaget till beslut.
[17] Avsnitt 1.1 i bilaga II till förslaget till beslut.

området uppgiftsskydd med skyddsåtgärder för alla enskilda personer, oavsett deras nationalitet, såsom PIPA. I detta sammanhang noterar dataskyddsstyrelsen att det i författningens artikel 6.2 fastställs att utländska medborgares ställning är garanterad i enlighet med internationella lagar och fördrag och den rättspraxis som nämns i förslaget till beslut, enligt vilken en ”utlänning” kan uppbära ”grundläggande rättigheter”. Med tanke på relevansen av erkännandet av ”utländska medborgares” rätt till uppgiftsskydd uppmärksammar dataskyddsstyrelsen kommissionen på nödvändigheten att fortsätta övervaka rättspraxisen för uppgiftsskydd som en grundläggande rättighet som inte bara tillerkänns sydkoreanska medborgare utan alla registrerade, för att säkerställa att den skyddsnivå för fysiska personer som garanteras i GDPR inte undergrävs vid överföring av personuppgifter till Sydkorea enligt beslutet om adekvat skyddsnivå.

3.1.1. Begrepp

45. På grundval av GDPR:s referensram för adekvat skyddsnivå bör grundläggande begrepp och/eller principer rörande uppgiftsskydd 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”[18].

46. PIPA innehåller ett antal definitioner, såsom avseende ”personuppgifter”, ”behandling” och ”registrerad”, som har stor likhet med de motsvarande termerna i GDPR.

3.1.1.1. Begreppet pseudonymiserade uppgifter

47. Bland definitionerna i PIPA fastställs särskilt i artikel 2.1 i PIPA personuppgifter som någon av följande information om en levande enskild person: a) information som identifierar en viss person genom dennes fullständiga namn, nummer i folkbokföringsregistret, bild, osv. samt b) information som, även om den inte i sig identifierar en viss person, lätt kan kombineras med annan information för att identifiera en viss person. Oavsett om lätthet att kombinera föreligger ska de senare fallen bestämmas genom att rimligen överväga den tid, kostnad, teknik, osv., som krävs för att identifiera den enskilda personen, såsom sannolikheten att den andra informationen kan inhämtas.

48. Dessutom, enligt artikel 2.1 c i PIPA anses ”pseudonymiserade uppgifter” också vara personuppgifter. Pseudonymiserade uppgifter definieras som information enligt post a) eller b) ovan som är pseudonymiserad enligt stycke 1–2 och därigenom inte förmår identifiera en viss person utan att informationen används eller kombineras för att återställa den i ursprungligt skick. Information som är fullständigt anonymiserad undantas från PIPA:s tillämpningsområde. Enligt artikel 58.2 i PIPA gäller lagen inte för information som inte längre identifierar en viss person när den kombineras med annan information, efter rimligt övervägande av tid, kostnad, teknik, osv.

49. Europeiska kommissionen hävdar i skäl 17 i sitt förslag till beslut att detta motsvarar GDPR:s materiella tillämpningsområde och dess begrepp ”personuppgifter”, ”pseudonymisering” och ”anonymiserad information”.

50. Men enligt artikel 28.7 i PIPA gäller artiklarna 20, 21, 27, 34.1, 35–37, 39.3, 39.4, 39.6–39.8 inte för pseudonymiserade personuppgifter.

51. I sitt förslag till beslut hävdar kommissionen att artikel 28.7 i PIPA endast är tillämplig på pseudonymiserade personuppgifter när de behandlas för ändamål som hänför sig till statistik,

[18] WP254, s. 4.

vetenskaplig forskning eller arkivering i det allmännas intresse[19]. Detta följer dock inte direkt av lagens bokstav utan av de förklaringar som ges i meddelande nr 2021-1[20]. Samtidigt som dataskyddsstyrelsen är medveten om att det, utifrån PIPA:s utformning och syfte, kan göras gällande att artikel 28.2 i PIPA bör förstås och logiskt tolkas som att den även gäller för artikel 28.7 i PIPA, uppmanar dataskyddsstyrelsen – mot bakgrund av vikten av meddelande nr 2021-1 i kommissionens bedömning av huruvida en adekvat skyddsnivå upprätthålls för personuppgifter i Republiken Korea samt för att undanröja alla tvivel – kommissionen att lämna ytterligare information om den bindande karaktären, verkställbarheten och giltigheten av meddelande nr 2021-1 och att övervaka dess tillämpning i detta specifika sammanhang.

52. I detta sammanhang vill dataskyddsstyrelsen erinra om att pseudonymisering enligt GDPR förstås som en rekommenderad säkerhetsåtgärd. Enligt GDPR förblir pseudonymiserade uppgifter därför personuppgifter, för vilka GDPR är fullständigt tillämplig. Utifrån det föregående befarar dataskyddsstyrelsen att GDPR:s nivå av skydd för pseudonymiserade personuppgifter kan undergrävas när personuppgifter överförs till Sydkorea. Dataskyddsstyrelsen uppmanar därför kommissionen att närmare bedöma effekten av pseudonymisering enligt PIPA och – allra viktigast – hur den kan påverka de grundläggande rättigheterna och friheterna för de registrerade vars personuppgifter skulle överföras till Republiken Korea på grundval av beslutet om adekvat skyddsnivå. Dataskyddsstyrelsen uppmanar därför kommission att lämna försäkringar om att skyddsnivån för personuppgifter från registrerade inom EES inte kommer att sänkas efter att de överförts till Republiken Korea också när de överförda personuppgifterna pseudonymiseras.

3.1.1.2. *Begreppet personuppgiftsansvarig*

53. I artikel 2.5 i PIPA definieras ”personuppgiftsansvarig” som en offentlig institution, juridisk person, organisation eller enskild person, osv., som behandlar personuppgifter direkt eller indirekt för att sköta register med personuppgifter ”som del av sin verksamhet”. I de ytterligare skyddsåtgärderna i meddelande nr 2021-1 definieras dock termen personuppgiftsansvarig som en offentlig institution, juridisk person, organisation, enskild person, osv., som behandlar personuppgifter direkt eller indirekt för att sköta registren med personuppgifter ”i företagssyfte”. I fotnot 272 i förslaget till beslut anges istället följande om begreppet *personuppgiftsansvarig*: ”Enligt definitionen i artikel 2 i PIPA, dvs. en offentlig institution, juridisk person, organisation, enskild person, osv., som behandlar personuppgifter direkt eller indirekt för att sköta register med personuppgifter ’i officiellt syfte eller företagssyfte’.”

54. Dataskyddsstyrelsen medger att dessa inkonsekvenser kan bero på översättningar av ursprungstexten som tillhandahållits av de sydkoreanska myndigheterna och uppmanar kommissionen att regelbundet kontrollera översättningarnas kvalitet och tillförlitlighet. Dataskyddsstyrelsen betonar dock att en klar förståelse av de ändamål för behandling som omfattas av PIPA:s materiella tillämpningsområde är nödvändig för att kunna bedöma den väsentligen likvärdiga skyddsnivån för uppgifter i den sydkoreanska rättsliga ramen. I detta sammanhang noterar dataskyddsstyrelsen att PIPA inte använder samma terminologi som i GDPR för begreppet ”personuppgiftsansvarig” och ”personuppgiftsbiträde”, och uppmanar därför kommissionen att klargöra den korrekta definitionen och tillämpningsområdet för begreppet ”personuppgiftsansvarig” och att särskilt förklara om denna term också omfattar personuppgiftsbiträden i den mening som avses i GDPR, eftersom detta direkt påverkar tillämpningsområdet för beslutet om adekvat skyddsnivå[21].

[19] Se bland annat skäl 82 i förslaget till beslut.
[20] Avsnitt 4 i bilaga I till förslaget till beslut.
[21] Se även punkt 38 ovan.

3.1.2. Delvisa undantag som medges i PIPA

55. I artikel 58.1 i PIPA undantas tillämpningen av delar av PIPA (dvs. artiklarna 15–57) för fyra kategorier av personuppgiftsbehandling, såsom beskrivs nedan. Undantagen gäller särskilt för bestämmelserna i PIPA om specifika skäl för behandling av personuppgifter, vissa skyldigheter avseende uppgiftsskydd, de utförliga reglerna för utövandet av individuella rättigheter samt reglerna för tvistlösning. Dataskyddsstyrelsen noterar dock att vissa allmänna bestämmelser i PIPA fortfarande är tillämpliga, t.ex. bestämmelserna om dataskyddsprinciperna (artikel 3 i PIPA) och individuella rättigheter (artikel 4 i PIPA). I artikel 58.4 i PIPA fastställs det dessutom specifika skyldigheter för dessa fyra kategorier av personuppgiftsbehandling.

56. För det första omfattar det delvisa undantaget personuppgifter som insamlats i enlighet med statistiklagen för behandling av offentliga institutioner. Europeiska kommissionen hävdar i skäl 27 i sitt förslag till beslut att det i förtydliganden som mottagits från den sydkoreanska regeringen görs gällande att personuppgifter som behandlas i detta sammanhang normalt avser sydkoreanska medborgare och endast i undantagsfall omfattar information avseende utlänningar, dvs. i de statistiska uppgifterna om inresa till och utresa från territoriet, eller avseende utländska investeringar. Enligt förslaget till beslut överförs dock inte normalt sådana data, ens i dessa situationer, från personuppgiftsansvariga/personuppgiftsbiträden inom EES, utan samlas snarare in direkt av offentliga myndigheter i Sydkorea.

57. Dataskyddsstyrelsen bekräftar kommissionens slutledning om de särskilda omständigheterna för tillämpningen av statistiklagen för behandling av personuppgifter som överförts enligt beslutet om adekvat skyddsnivå. Dataskyddsstyrelsen välkomnar dock ytterligare information och garantier om de specifika skyddsåtgärder som skulle tillämpas ifall personuppgifter som överförts från EES insamlas vidare i enlighet med statistiklagen för behandling av offentliga institutioner, särskilt vad gäller de registrerades utövande av individuella rättigheter i linje med artikel 89.2 i GDPR i den utsträckning som sådana rättigheter sannolikt inte kommer att omöjliggöra eller allvarligt försvåra uppfyllandet av de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

58. I detta perspektiv verkar tillämpningen av artikel 4 i PIPA att tillhandahålla garantier också för denna typ av behandling. Dataskyddsstyrelsen välkomnar dock ytterligare information och förtydliganden i beslutet om adekvat skyddsnivå om de specifika skyldigheter som fastställs, i enlighet med artikel 58.4 i PIPA, om dessa uppgiftsbehandlingar, dvs. avseende uppgiftsminimering, begränsad lagring av uppgifter, säkerhetsåtgärder och hantering av klagomål.

59. För det andra omfattar det delvisa undantaget personuppgifter som insamlats eller begärts att tillhandahållas för analysen av information om nationell säkerhet. Dataskyddsstyrelsen är medveten om att stater i ärenden som rör nationell säkerhet utövar en bred skönsmässig bedömning som erkänns av Europeiska domstolen för de mänskliga rättigheterna. Dataskyddsstyrelsen noterar att artikel 37.2 i den sydkoreanska författningen gör gällande att en begränsning av friheter och rättigheter, till exempel när så krävs för att skydda den nationella säkerheten, inte behöver åsidosätta den väsentliga aspekten av denna frihet eller rättighet. Vidare noterar dataskyddsstyrelsen skyddsåtgärderna i avsnitt 6 i meddelande nr 2021-1 avseende behandlingen av personuppgifter för ändamål som hänför sig till nationell säkerhet, däribland undersökning av överträdelser och verkställighet. I samband med detta uppmanar dock dataskyddsstyrelsen kommissionen att närmare förtydliga tillämpningsområdet för undantagen, eftersom den frågar sig om samtliga undantag som lämnas enligt artikel 58.1 2 i PIPA (kapitlen III–VII) är relevanta för underrättelsetjänsternas arbete, och om de tillser likvärdighet med principerna om nödvändighet och proportionalitet. Dataskyddsstyrelsen uppmanar kommissionen särskilt till att lämna fler förtydliganden avseende under vilka omständigheter en underrättelsetjänst kan förlita sig på undantagen. Dataskyddsstyrelsen finner det nödvändigt att noga övervaka effekten av dessa begränsningar i praktiken, särskilt vad gäller det effektiva utövandet och verkställandet av de registrerades rättigheter.

60. För det tredje gäller det delvisa undantaget för ”personuppgifter som tillfälligt behandlas när det är av yttersta vikt på grund av allmän säkerhet och trygghet, hälsa, osv.” Enligt skäl 29 i kommissionens förslag till beslut tolkas denna kategori strikt av PIPC och gäller endast i nödsituationer som kräver omedelbara insatser, till exempel för att spåra infektiösa agens, eller rädda och bistå offer för naturkatastrofer.

61. Dataskyddsstyrelsen betonar dessutom att alla undantag från skyddsnivån för personuppgifter bör tolkas strikt. Samtidigt noterar dataskyddsstyrelsen att bestämmelsen inte är strikt definierad och inte tillhandahåller en uttömmande förteckning över exempel på situationer när behandlingen av personuppgifter skulle kunna anses vara ”av yttersta vikt”. Dataskyddsstyrelsen hyser t.ex. farhågor över huruvida internationella överföringar av hälsouppgifter under den pågående covid-19-pandemin också skulle omfattas av tillämpningsområdet för detta undantag. Dataskyddsstyrelsen uppmanar därför kommissionen att lämna ytterligare klargöranden om tillämpningsområdet för detta undantag och att fullt ut övervaka dess tillämpning och tillämpningsområde för att tillse att det inte leder till en sänkt skyddsnivå för personuppgifter från EES efter deras överföring till Sydkorea på grundval av beslutet om adekvat skyddsnivå.

62. Slutligen gäller det delvisa undantaget för personuppgifter som insamlas eller används för ändamål som hänför sig till pressrapportering, religiösa organisationers missionsverksamhet, och politiska partiers nominering av kandidater[22]. Vad gäller pressens behandling av personuppgifter i journalistiskt syfte hävdar kommissionen i skäl 31 i sitt förslag till beslut att balansen mellan uttrycksfrihet och andra rättigheter, såsom rätten till personlig integritet, tillerkänns av lagen om skiljedomsförfarande och påföljder, osv. för skada orsakad av pressmeddelanden (nedan kallat *presslagen*), och ställer upp specifika skyddsåtgärder som följer av presslagen. Dataskyddsstyrelsen uppmanar dock kommissionen att fullt ut övervaka detta undantag och relevant rättspraxis för att tillse att en likvärdig nivå av uppgiftsskydd också säkerställs i praktiken i den sydkoreanska rättsliga ramen.

3.1.3. Grunder för laglig och rättvis behandling för berättigade ändamål

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

64. Genom en liknande struktur som GDPR presenteras i PIPA inledningsvis först principen om laglighet, rättvisa och öppenhet (artikel 3.1–3.2 i PIPA), och därefter fastställningen av de specifika reglerna för dess tillämpning (artiklarna 15–19 i PIPA). Artikel 15 i PIPA innehåller en katalog över rättsliga grunder på vilka de personuppgiftsansvariga kan basera insamlingen av personuppgifter och använda den inom tillämpningsområdet för ändamålet för insamling. Dessa rättsliga grunder består av 1) den registrerades informerade samtycke; 2) tillstånd enligt lag eller nödvändighet att fullgöra en rättslig förpliktelse; 3) nödvändighet att utföra en offentlig institutions skyldigheter; 4) nödvändighet att genomdriva eller genomföra ett avtal med en registrerad; 5) nödvändighet att skydda den registrerades liv eller en tredje parts liv, kroppsliga eller egendomsrelaterade intressen mot överhängande fara (och föregående samtycke kan inte erhållas); 6) nödvändighet att uppnå en personuppgiftsansvarigs berättigade intresse som överträffar den registrerades.

65. I artikel 17 i PIPA förtecknas dessutom de rättsliga grunderna för utbyte av personuppgifter med en tredje part, som innefattar 1) den registrerades informerade samtycke; 2) tillstånd enligt lag eller

[22] Religiösa organisationers behandling av personuppgifter för sin missionsverksamhet och politiska partiers behandling av personuppgifter i samband med nomineringen av kandidater är också undantagna från tillämpningsområdet för beslutet om adekvat skyddsnivå. Se även punkt 37 ovan i avsnitt 2.3.2.

nödvändighet att fullgöra en rättslig förpliktelse; 3) nödvändighet att utföra en offentlig institutions skyldigheter; och 4) nödvändighet att skydda den registrerades liv eller en tredje parts liv, kroppsliga eller egendomsrelaterade intressen mot överhängande fara (och föregående samtycke kan inte erhållas). Också i avsaknad av den registrerades samtycke tillåts utbyte av personuppgifter när så sker inom ett tillämpningsområde som är rimligen relaterat till de ändamål som personuppgifterna ursprungligen insamlades för (artikel 17.4 i PIPA).

66. I artikel 18 i PIPA fastställs specifika regler för användningen och utbytet av personuppgifter när så sker utanför tillämpningsområdet för det ursprungliga ändamålet för insamling eller tillhandahållande. Också här är samtycke en sådan tillståndsregel.

67. Samtidigt som dataskyddsstyrelsen erkänner den stora likheten mellan sydkoreansk lagstiftning och GDPR vad gäller principen om laglighet och närvaron av en allmän rätt till upphävande (artikel 37 i PIPA), som också kan åberopas när personuppgifter behandlas på grundval av samtycke, noterar dataskyddsstyrelsen att det i PIPA saknas en allmän rätt att återkalla sitt samtycke[23]. Mot bakgrund av samtyckets betydelse som rättslig grund i alla scenarier som beskrivs ovan, och med beaktande av den roll som individuella rättigheter intar i ett rättsligt system för uppgiftsskydd för att skydda de registrerades grundläggande rättigheter och friheter, uppmanar dataskyddsstyrelsen kommissionen att närmare bedöma effekten av avsaknaden av en allmän rätt att återkalla sitt samtycke enligt sydkoreansk lagstiftning och att lämna ytterligare försäkringar för att säkerställa att en väsentlig nivå av uppgiftsskydd som den som säkerställs enligt GDPR alltid garanteras, också genom att vid behov förtydliga den roll som rätten till upphävande intar i detta specifika sammanhang.

3.1.4. Principen om ändamålsbegränsning

68. Enligt GDPR:s referensram för adekvat skyddsnivå ska personuppgifter, i linje med GDPR, behandlas för ett specifikt ändamål och därefter endast utnyttjas i den mån detta inte är oförenligt med behandlingens ändamål.

69. I enlighet med artiklarna 3.1 och 3.2 i PIPA ska de personuppgiftsansvariga specificera och uttryckligen ange behandlingens ändamål och säkerställa att behandlingen är förenlig med dessa ändamål. Denna princip bekräftas i andra bestämmelser (dvs. artiklarna 15.1, 18.1 och 19.1 i PIPA), men behandling för ”rimligen relaterade” ändamål är under vissa omständigheter ändå tillåten (se artikel 17.4 i PIPA)[24] liksom användning och tillhandahållande av personuppgifter utanför ändamålet (se artiklarna 18 och 19 i PIPA)[25].

70. Vid överföringar av personuppgifter från EES till Republiken Korea på grundval av beslutet om adekvat skyddsnivå förstår dataskyddsstyrelsen att ändamålet för de EES-baserade personuppgiftsansvarigas insamling utgör det ändamål för vilket uppgifterna överförs för behandling av den mottagande personuppgiftsansvarige baserad i Sydkorea. En ändring av ändamålet av den personuppgiftsansvarige baserad i Sydkorea skulle endast tillåtas i enlighet med artiklarna 18.2. 1–3 i

[23] Även om registrerade i vissa fall kan neka samtycke, se t.ex. artikel 18.3 5 i PIPA. Rätten att återkalla sitt samtycke verkar dock bara finnas i vissa specifika fall. I enlighet med artikel 27.1 2 i PIPA har de registrerade rätt att återkalla sitt samtycke när de inte önskar att deras personuppgifter överförs till en tredje part på grund av överföringen av en del av, eller hela, den personuppgiftsansvariges företag, en fusion, osv. I enlighet med artikel 39.7 i PIPA kan användare när som helst återkalla sitt samtycke till insamling, användning och tillhandahållande av personuppgifter från leverantörer av informations- och kommunikationstjänster, osv. Och i enlighet med artikel 37 i CIA kan en enskild person som omfattas av kreditupplysning återkalla samtycke som lämnats till en leverantör/användare av kreditupplysningar.

[24] Varvid ändamålets förenlighet måste avgöras i förväg på grundval av de kriterier som fastställs i artikel 14–2 i PIPA:s genomförandeförordning.

[25] Se även punkt 66 ovan.

PIPA, ”om inte detta sannolikt otillbörligt åsidosätter den registrerades eller en tredje parts intressen”[26]. I detta sammanhang bekräftar dataskyddsstyrelsen kommissionens yttrande i skäl 55 i förslaget till beslut att där ändringar av ändamålet är tillåtna enligt lag, måste sådana lagar respektera den grundläggande rätten till personlig integritet och uppgiftsskydd. Dataskyddsstyrelsen noterar dock att ingen specifik information har lämnats för att underbygga detta särskilda yttrande, till exempel saknas hänvisning till artikel 37 i den (sydkoreanska) författningen. Dataskyddsstyrelsen uppmanar därför kommissionen att lämna ytterligare försäkringar och garantier i förslaget till beslut för att tillse att eventuella lagar som tillåter en ändring av ändamålet för behandling måste respektera de registrerades grundläggande rättigheter och friheter avseende personlig integritet och uppgiftsskydd.

3.1.5. Principen om uppgifternas kvalitet och proportionalitet

71. Enligt GDPR:s referensram för adekvat skyddsnivå ska personuppgifter vara riktiga och om nödvändigt hållas uppdaterade. Personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål som de behandlas för.

72. Enligt PIPA måste de personuppgiftsansvariga tillse att personuppgifterna är riktiga, fullständiga och uppdaterade i den utsträckning som är nödvändig i förhållande till de ändamål som personuppgifterna behandlas för (artikel 3.3 i PIPA). De personuppgiftsansvariga ska samla in så lite personuppgifter som behövs för att uppnå ett visst ändamål. De uppbär bevisbördan i detta hänseende (artikel 16.1 i PIPA).

73. I detta avseende delar dataskyddsstyrelsen därför kommissionens bedömning vad gäller den väsentligen likvärdiga skyddsnivån i PIPA jämfört med GDPR.

3.1.6. Principen om lagring av uppgifter

74. Enligt GDPR:s referensram för adekvat skyddsnivå och som allmän regel ska inte uppgifter lagras längre än nödvändigt för de ändamål som personuppgifterna behandlas för. Enligt artikel 21.1 i PIPA finns denna princip också i sydkoreansk lagstiftning. Enligt PIPA måste de personuppgiftsansvariga utan dröjsmål förstöra personuppgifterna när de blir överflödiga vid utgången av deras tid för lagring eller när det avsedda ändamålet med behandlingen har uppnåtts, om inte en lagstadgad tid för att spara personuppgifter gäller.

75. Dataskyddsstyrelsen finner det dock oroande att artikel 21.1 i PIPA inte är tillämplig på pseudonymiserade personuppgifter. Dataskyddsstyrelsen noterar dock följande, enligt avsnitt 4 iii i meddelande nr 2021-1: ”när en personuppgiftsansvarig behandlar pseudonymiserade uppgifter för sammanställning av statistik, vetenskaplig forskning, bevarande av offentliga register, osv., och om den pseudonymiserade informationen inte har förstörts efter att det specifika ändamålet med behandlingen har uppfyllts i linje med artikel 37 i författningen och artikel 3 (principer för skydd av personuppgifter) i lagen, ska denne anonymisera informationen för att säkerställa att den inte längre identifierar en viss person, ensam eller kombinerad med annan information, med rimlig tanke på tid, kostnad, teknik, osv., i enlighet med artikel 58.2 i PIPA.” Då meddelande nr 2021-1 är av stor betydelse, och för att uppnå rättssäkerhet vad gäller den likvärdiga skyddsnivån för personuppgifter som överförs till Republiken Korea enligt beslutet om adekvat skyddsnivå, upprepar dataskyddsstyrelsen sin uppmaning till kommissionen att lämna ytterligare information som specifikt tar upp hur meddelande nr 2021-1 görs bindande och hur dess verkställbarhet och giltighet säkerställs[27].

[26] Artikel 18.2 i PIPA.

[27] Se även punkt 51 ovan, under avsnitt 3.1.1.1 i detta yttrande, samt punkt 52 vad gäller dataskyddsstyrelsens allmänna farhågor över effekten av pseudonymisering enligt sydkoreansk lagstiftning.

3.1.7. Principen om säkerhet och konfidentialitet

76. Såsom beskrivs i GDPR:s referensram för adekvat skyddsnivå kräver principen om säkerhet och konfidentialitet att enheter som behandlar personuppgifter säkerställer att personuppgifterna behandlas på ett sätt som garanterar deras säkerhet, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, genom att använda lämpliga tekniska eller organisatoriska åtgärder. Säkerhetsnivån bör beakta den senaste tekniska utvecklingen och de relaterade kostnaderna.

77. Europeiska kommissionen har identifierat en liknande princip om datasäkerhet i artikel 3.4 i PIPA, som närmare bestäms i artikel 29 i PIPA. Dessutom gäller bestämmelser om datasäkerhet när den personuppgiftsansvarige anlitar en ”entreprenör”. Behandlingens säkerhet måste garanteras genom tekniska skyddsåtgärder och skyddsåtgärder på ledningsnivå, som också måste ingå i det bindande avtalet om behandling av personuppgifter (artikel 26 i PIPA och artikel 28 i PIPA:s genomförandeförordning). När en personuppgiftsöverträdelse sker gäller vidare specifika skyldigheter enligt PIPA, inräknat skyldigheten att meddela drabbade registrerade och tillsynsmyndigheten ifall antalet drabbade registrerade överstiger det tillämpliga tröskelvärdet (artikel 34 i PIPA sammantaget med artikel 39 i PIPA:s presidentdekret), förutom om de berörda uppgifterna är pseudonymiserade personuppgifter som behandlas för ändamål som hänför sig till statistik, vetenskaplig forskning eller arkivering i det allmännas intresse (artikel 28.7 i PIPA). Också här[28] hyser dataskyddsstyrelsen farhågor över de långtgående undantagen för pseudonymiserade uppgifter och uppmanar kommissionen återigen att närmare bedöma denna aspekt för att tillse att en väsentligen likvärdig nivå av uppgiftsskydd säkerställs enligt sydkoreansk lagstiftning[29].

78. Sammanfattningsvis accepterar dataskyddsstyrelsen ändå kommissionens bedömning och slutsats angående den sydkoreanska lagstiftningens väsentliga likvärdighet med principen om säkerhet och konfidentialitet.

3.1.8. Öppenhetsprincipen

79. På grundval av artikel 5.1 a i GDPR är öppenhet en grundläggande princip i EU:s system för skydd av personuppgifter. Skäl 39 i GDPR beskriver den avgörande funktionen hos denna princip genom att hävda att ”[d]et bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. [...] Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen.”

80. I GDPR:s referensram 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. Mer specifikt hävdar den att ”varje enskild person bör informeras om samtliga huvuddrag i behandlingen av hans/hennes personuppgifter i en klar, lätt tillgänglig, koncis, öppen och begriplig form. Sådan information bör innehålla ändamålet med behandlingen, den personuppgiftsansvariges identitet, de rättigheter som görs tillgängliga för honom/henne och annan information om så är nödvändigt för att rättvisa ska garanteras. *Such information should include the purpose of the processing, the identity of the data controller, the rights made available to him/her and other information insofar as this is necessary to ensure fairness.* Under vissa förhållanden kan det finnas vissa undantag från denna rätt till information, till exempel för att skydda brottsundersökningar, nationell säkerhet, rättsligt oberoende och rättsliga förfaranden eller andra viktiga ändamål av allmänt intresse som är fallet med artikel 23 i GDPR.”

[28] Som redan fastställts i punkterna 51–52 ovan och i avsnitt 3.1.1.1 i detta yttrande.
[29] Se även avsnitten 3.1.6 och 3.1.10 i detta yttrande.

81. Liksom GDPR innehåller PIPA en allmän öppenhetsprincip som kräver att de personuppgiftsansvariga offentliggör sin integritetspolicy och andra frågor som är förknippade med behandling av personuppgifter (artikel 3.5 i PIPA). Specifika informationsskyldigheter gäller när de personuppgiftsansvariga söker erhålla de registrerades samtycke för insamling och behandling av personuppgifter (artikel 15.2 i PIPA), för utbyte av personuppgifter med en tredje part (artikel 17.2 i PIPA) och för behandling utanför ändamålet (artikel 18.3 i PIPA). Det är värt att notera att dessa informationsskyldigheter också gäller för entreprenören efter nödvändiga ändringar (artikel 26.7 i PIPA).

82. Dataskyddsstyrelsen erkänner och välkomnar de ytterligare skyddsåtgärder som anges i avsnitt 3.i och ii i meddelande nr 2021-1[30] rörande information som de registrerade ska tillhandahållas när en EES-enhet överför deras uppgifter och förstår att de registrerade, i enlighet med artikel 20.1 i PIPA, endast informeras på begäran när uppgifter inte har erhållits från de registrerade. En allmän rätt att bli informerad erkänns nämligen endast i enlighet med artikel 20.2 i PIPA när vissa behandlingar överstiger tröskelvärdena i PIPA:s genomförandeförordning (artikel 15.2).

83. Totalt sett accepterar dataskyddsstyrelsen att skyddsnivån i sydkoreansk lagstiftning vad gäller öppenhetsprincipen är väsentligen likvärdig med den som tillhandahålls i GDPR.

3.1.9. Särskilda kategorier av personuppgifter

84. För att ett tredjelands system för skydd av personuppgifter ska anses tillhandahålla en skyddsnivå för personuppgifter som är väsentligen likvärdig med den i GDPR ska specifika skyddsåtgärder finnas på plats vid involveringen av särskilda kategorier av personuppgifter i den mening som avses i artiklarna 9 och 10 i GDPR.

85. Enligt PIPA gäller specifika bestämmelser för behandlingen av s.k. känslig information, i vilken ingår personuppgifter som avslöjar ideologi, troslära, inträde i eller utträde ur en fackförening eller ett politiskt parti, politiska åsikter, hälsa, sexliv och andra personuppgifter som sannolikt kraftigt hotar alla registrerades integritet, liksom, med hänvisning till PIPA:s genomförandeförordning, DNA-information som förvärvats genom genetisk testning, uppgifter ur ett brottsregister; personuppgifter som hänför sig till specifik teknisk behandling av uppgifter rörande en enskild persons fysiska, fysiologiska eller beteendemässiga kännetecken i syfte att identifiera honom eller henne enskilt; samt personuppgifter som avslöjar ras eller etniskt ursprung.

86. Liksom i GDPR är behandling av känslig information förbjudet enligt sydkoreansk dataskyddslag om inte specifika undantag gäller, bestående av 1) att den registrerade informeras och ett specifikt samtycke erhålls, och 2) rättsliga bestämmelser som tillåter behandlingen (artikel 23.2 i PIPA).

87. På denna grundval tillstyrkte dataskyddsstyrelsen i princip kommissionens slutsats om den sydkoreanska lagstiftningens väsentliga likvärdighet vad gäller behandlingen av särskilda kategorier av personuppgifter. Dataskyddsstyrelsen vill dock notera att den inte har erhållit PIPA:s manual eller förtydligandena från PIPC avseende huruvida tolkningen av termen ”sexualliv” också inkluderar den enskilda personens sexuella orientering eller läggning, vilka inte har inkluderats i meddelande nr 2021-1. Dataskyddsstyrelsen uppmanar därför kommissionen att tillhandahålla denna information för att kunna göra en oberoende bedömning av den. Vidare uppmanar dataskyddsstyrelsen kommissionen att specifikt citera de handlingar där den information som hänvisas till i detta ämne kan hittas.

3.1.10. Rätt till tillgång, rättelse, utplåning och rätt att göra invändningar

88. I den sydkoreanska rättsliga ramen erkänns de registrerades rättigheter i artikel 3.5 i PIPA – enligt vilken den personuppgiftsansvarige ska garantera de registrerades rättigheter som förtecknas i

[30] Bilaga I till förslaget till beslut.

artikel 4 i PIPA och närmare bestäms i artiklarna 35–37, 39 och 39.2 i PIPA och, vad gäller ”personliga kreditupplysningar” (dvs. ”kreditupplysningar som är information som krävs för att avgöra kreditvärdigheten för parter till finansiella eller kommersiella transaktioner – se skäl 3 i förslaget till beslut), i artiklarna 37, 38, 38.3 i CIA.

89. Dataskyddsstyrelsen noterar att rätten till tillgång (och till rättelse och utplåning som kan utövas av en ”registrerad som har tillgång till sina personuppgifter i enlighet med artikel 35 i PIPA) kan begränsas eller nekas ”när tillgång förbjuds eller begränsas enligt lag”, ”när tillgång kan orsaka skada på en tredje parts liv eller kropp, eller omotiverat intrång i en annan persons egendom eller andra intressen”, och dessutom, för offentliga institutioner, när beviljandet av tillgång ”skulle göra det mycket svårt” att utföra vissa funktioner, som närmare bestäms i artikel 35.4 i PIPA[31]. Liknande bestämmelser finns också i artikel 37 i PIPA gällande rätten att upphäva behandlingen av personuppgifter.

90. Genom artikel 23 i GDPR kan unionsrätten eller medlemsstaternas nationella rätt begränsa individuella rättigheter när en sådan begränsning respekterar det väsentliga innehållet i de grundläggande rättigheterna och friheterna och är en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle, där sådana begränsningar föreskrivs för att t.ex. säkerställa skyddet av den registrerade eller andra personers rättigheter och friheter och ”en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i fall som nämns i a–e och g” i samma artikel.

91. Dataskyddsstyrelsen välkomnar därför allmänna garantier i förslaget till beslut om att det behövs en lag eller stadga som begränsar de registrerades rättigheter att uppfylla kraven i den sydkoreanska författningen att en grundläggande rättighet endast får begränsas när så behövs för den nationella säkerheten, eller upprätthållandet av lag och ordning för den allmänna välfärden, och att denna begränsning inte får påverka den berörda frihetens eller rättighetens väsentliga innehåll (artikel 37.2 i den sydkoreanska författningen).

92. Vad gäller undantaget i samband med ”ett omotiverat intrång i en annan persons egendom eller andra intressen”, medger dataskyddsstyrelsen vidare att detta ”innebär en balansering mellan de konstitutionellt skyddade rättigheterna och friheterna för, å ena sidan, den enskilda personen och, å andra sidan, för andra personer”[32]. Dataskyddsstyrelsen uppmanar dock kommissionen att fullt ut övervaka tillämpningen av detta undantag och relevant rättspraxis för att tillse att en likvärdig nivå av uppgiftsskydd i den sydkoreanska rättsliga ramen också säkerställs i praktiken.

93. På samma sätt välkomnar dataskyddsstyrelsen en noggrann övervakning av tillämpningen av undantaget för de offentliga organen, särskilt vad gäller de fall där det skulle anses att beviljandet av tillgång gör det ”mycket svårt” att utföra deras uppdrag med tanke på att detta uttryck verkar vara bredare än det som används i andra bestämmelser i PIPA, t.ex. i artikel 18.2 5[33], och bör tolkas restriktivt för att undvika orimliga begränsningar av de registrerades rättigheter.

94. Dataskyddsstyrelsen hyser dessutom farhågor över huruvida undantagen, enligt vilka bestämmelserna om öppenhet på begäran (artikel 20 i PIPA) och individuella rättigheter (artiklarna 35–37 i PIPA) – samt de liknande bestämmelserna om kraven på leverantörer av informations- och kommunikationstjänster (artiklarna 39.2, 39.6–39.8 i PIPA) och de som ingår i CIA (se undantagen enligt artikel 40.3 i CIA) – inte gäller när det rör sig om pseudonymiserade uppgifter,

[31] Samma villkor och undantag för rätten till tillgång och korrektion som ges enligt PIPA gäller också avseende den rätt till tillgång och korrektion som ges för personliga kreditupplysningar enligt CIA (fotnot 135 i förslaget till beslut).

[32] Skäl 76 i förslaget till beslut.

[33] Vad gäller undantagen från begränsningen av användning och tillhandahållande av personuppgifter utanför ändamålet, hänvisar artikel 18.2 5 i PIPA till situationer där offentliga institutioner ”finner det omöjligt” att utföra sitt uppdrag.

när dessa behandlas för ändamål som hänför sig till statistik, vetenskaplig forskning eller arkivering i det allmännas intresse (artikel 28.7 i PIPA), överensstämmer med de skyddsåtgärder som föreskrivs i den europeiska rättsliga ramen.

95. Dessa bestämmelser verkar införa ett allmänt undantag för en sådan typ av behandling medan det i GDPR anges att – i de fall där personuppgifter (inräknat pseudonymiserade personuppgifter) behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål – unionsrätten eller medlemsstaternas nationella rätt kan fastställa undantag från de registrerades rättigheter, men endast ”i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål”, där pseudonymisering bara är en av de tekniska och organisatoriska åtgärder som ska antas för att tillse respekten för principen om uppgiftsminimering (artikel 89.1 i GDPR).

96. Europeiska kommissionen anser att det undantag som anges i artikel 28.7 i PIPA även är motiverat mot bakgrund av artikel 28.5 i PIPA, genom vilken den personuppgiftsansvarige uttryckligen förbjuds att behandla de pseudonymiserade uppgifterna för att identifiera en viss person och hänvisar till metoden i artikel 11.2 i GDPR (sammantaget med skäl 57 i GDPR) för behandling som inte kräver identifiering[34].

97. Faktum är att den personuppgiftsansvarige enligt artikel 11 i GDPR inte ska vara tvungen att ”bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade” endast i syfte att följa GDPR om den, för de avsedda ändamålen, kan behandla personuppgifter som inte kräver, eller inte längre kräver, att en registrerad identifieras. I dessa fall, när den personuppgiftsansvarige förmår visa att den inte är i stånd att identifiera den registrerade, gäller inte registrerades rättigheter. Såsom kommissionen bekräftar[35], krävs det i GDPR därför, i sådana fall, en ”praktisk” omöjlighet för den personuppgiftsansvarige och, i enlighet med principen om uppgiftsminimering, bekräftas det i GDPR att inga ytterligare uppgifter måste behandlas ”på grund av” GDPR.

98. Dataskyddsstyrelsen finner dock att denna situation skiljer sig från den där en personuppgiftsansvarig praktiskt taget är i stånd att identifiera den registrerade men inte tillåts detta på grund av en bestämmelse såsom den i artikel 28.5 i PIPA. I detta sammanhang välkomnar dataskyddsstyrelsen de förtydliganden som PIPC lämnat i meddelande nr 2021-1[36] och bekräftar att avsnitt 3 i PIPA (inräknat artikel 28.7) och undantaget i artikel 40.3 i CIA endast gäller när pseudonymiserade uppgifter behandlas för ändamål som hänför sig till vetenskaplig forskning, statistik eller arkivering i det allmännas intresse. Som tillägg till de redan nämnda farhågorna över den bindande karaktären av meddelande nr 2021-1[37] undrar dock dataskyddsstyrelsen fortfarande om de undantag som anges i artikel 28.7 i PIPA och artikel 40.3 i CIA kan anses vara nödvändiga och proportionerliga i ett demokratiskt samhälle i den mån de begränsar den registrerades rättigheter i samtliga fall där pseudonymiserade uppgifter behandlas för sådana ändamål – dvs. också när den personuppgiftsansvarige praktiskt taget är i stånd att identifiera den registrerade och rättigheterna sannolikt inte kommer att omöjliggöra eller allvarligt försvåra uppfyllandet av de särskilda ändamålen.

99. I synnerhet befarar dataskyddsstyrelsen att dessa undantag inte skulle vara motiverade och skulle behöva undersökas närmare, särskilt om de tillämpas av den personuppgiftsansvarige som

[34] Det ska noteras att samma slutledning inte skulle vara tillämplig som sådan på undantaget enligt artikel 40.3 i CIA för behandlingen av pseudonymiserade personuppgifter eftersom det i artikel 40.2 6 anges att: ”Ett kreditupplysningsföretag, osv., ska inte behandla pseudonymiserade personuppgifter så att en specifik enskild person kan identifieras i vinstsyfte eller otillbörliga syften” och som därför kan möjliggöra ny identifiering för ett tillbörligt syfte, såsom att uppfylla en begäran från en registrerad.

[35] Se skäl 82 i förslaget till beslut.

[36] Avsnitt 4 i bilaga I till förslaget till beslut.

[37] Se avsnitt 3.1.1.1 ovan.

pseudonymiserar uppgifterna ”för ändamål som hänför sig till statistik, vetenskaplig forskning och arkivering i det allmännas intresse, osv.”, i enlighet med artikel 28.2 i PIPA ”utan de registrerades samtycke” (och utan att tillhandahålla information som anges i artikel 20 i PIPA)[38], i den mån denna personuppgiftsansvarige bevarar den information som medger den nya identifieringen. Enligt GDPR ska enskilda personer kunna utöva sina rättigheter med avseende på all information som kan identifiera eller skilja ut dem, också om informationen betraktas som ”pseudonymiserad” om inte den redan nämnda artikel 11 i GDPR gäller. Dataskyddsstyrelsen noterar därför att endast när dessa uppgifter lämnas till en tredje part för samma ändamål som hänför sig till statistik, vetenskaplig forskning eller arkivering, ska information som kan användas för att identifiera en viss person inte ingå. Därför skulle troligen bara den personuppgiftsansvarige till vilken pseudonymiserade uppgifter lämnas i enlighet med artikel 28-2.2 i PIPA vara ”praktiskt taget” ur stånd att identifiera den registrerade utan ytterligare information.

100. Sammanfattningsvis bekräftar kommissionen följande: ”istället för att förlita sig på pseudonymisering som en möjlig skyddsåtgärd, föreskriver PIPA den som en förutsättning för vissa behandlingar för ändamål som hänför sig till statistik, vetenskaplig forskning och arkivering i det allmännas intresse (såsom att kunna behandla uppgifterna utan samtycke eller kombinera olika dataset)”[39] men anger för sådana fall betydande begränsningar av de registrerades rättigheter. Dataskyddsstyrelsen uppmanar kommissionen att närmare bedöma undantagen i artikel 28.7 i PIPA och artikel 40.3 i CIA och att noga övervaka deras tillämpning och relevant rättspraxis[40] för att tillse att de registrerades rättigheter inte orimligen begränsas när personuppgifter som överförs enligt beslutet om adekvat skyddsnivå behandlas för dessa ändamål, med beaktande av att dessa rättigheter i många fall också hjälper den personuppgiftsansvarige att säkerställa de behandlade uppgifternas kvalitet.

3.1.11. Begränsningar för vidare överföring

101. I GDPR:s referensram för adekvat skyddsnivå klargörs det att skyddsnivån för fysiska personer vars personuppgifter överförs enligt beslutet om adekvat skyddsnivå inte får undergrävas av den vidare överföringen, varför all vidare överföring ”bara ska tillåtas om den ytterligare mottagaren (dvs. mottagaren av den vidare överföringen) också omfattas av regler (inräknat avtalsregler) som säkerställer en adekvat skyddsnivå och som följer de relevanta anvisningarna vid uppgiftsbehandling på uppdrag av den personuppgiftsansvarige”.

102. Vad gäller de vidare överföringarna till entreprenörer (dvs. ”personuppgiftsbiträden”) som har inrättats i andra tredjeländer, noterar dataskyddsstyrelsen att den sydkoreanska rättsliga ramen saknar särskilda regler som täcker dessa fall och att en sydkoreansk personuppgiftsansvarig, enligt kommissionens uppfattning[41], måste säkerställa överensstämmelse med PIPA:s bestämmelser om utläggning på entreprenad (artikel 26 i PIPA) genom ett rättsligt bindande instrument och kommer att ansvara för de personuppgifter som har lagts ut på entreprenad (artikel 26 i PIPA).

103. Vad gäller de vidare överföringarna till tredje parter (dvs. andra personuppgiftsansvariga), måste, enligt artikel 17.3 i PIPA, en sydkoreansk personuppgiftsansvarig informera de registrerade och erhålla deras samtycke till överföringarna till utlandet och ”ska inte teckna avtal för en gränsöverskridande överföring av personuppgifter som strider mot PIPA”. Dataskyddsstyrelsen noterar att denna sista

[38] Se artikel 28.7 i PIPA, såsom förklaras i meddelande nr 2021-1, enligt vilket vissa skyddsåtgärder i PIPA, dvs. ”artiklarna 20, 21, 27, 34.1, 35–37, 39.3, 39.4, 39.6–39.8” inte ska gälla för pseudonymiserade uppgifter som behandlas för sammanställning av statistik, vetenskaplig forskning, bevarande av offentliga register, osv.
[39] Skäl 42 i förslaget till beslut.
[40] Se t.ex. Open Nets konstitutionella utmaningar (information på https://opennet.or.kr/19909 finns endast på koreanska).
[41] Skäl 87 i förslaget till beslut

bestämmelse – enligt kommissionens uppfattning[42] – kommer att säkerställa att inget avtal för gränsöverskridande överföringar kan innehålla skyldigheter som motsäger PIPA:s krav på den personuppgiftsansvarige och därför kan betraktas som en skyddsåtgärd. Emellertid föreskriver den ingen skyldighet att införa skyddsåtgärder för att säkerställa att samma skyddsnivå som PIPA ger, också kommer att ges av mottagaren. Dataskyddsstyrelsen inser därför att den registrerades informerade samtycke i allmänhet kommer att användas som grund för uppgiftsöverföringar från en personuppgiftsansvarig baserad i Sydkorea till en tredjelandsbaserad mottagare.

104. De ytterligare förtydliganden som har lämnats av PIPC i meddelande nr 2021-1 vad gäller skyldigheten att informera enskilda personer om det tredjeland som deras uppgifter kommer att överföras till[43] är välkomna, eftersom detta – som kommissionen betonar[44] – skulle hjälpa de registrerade inom EES att fatta ett fullständigt informerat beslut om huruvida de ska samtycka till en överföring till utlandet eller inte.

105. Men som också övervägs i yttrande 28/2018 om Europeiska kommissionens förslag till genomförandebeslut om adekvat skydd av personuppgifter i Japan, har det betonats att de registrerade, enligt GDPR, måste uttryckligen informeras om de möjliga riskerna med sådana överföringar, till följd av avsaknaden av adekvat skydd i tredjelandet och avsaknaden av lämpliga skyddsåtgärder före samtycket. Ett sådant meddelande bör t.ex. innehålla information om att det kanske saknas en tillsynsmyndighet och/eller principer för behandling av uppgifter och/eller den registrerades rättigheter i tredjelandet[45]. För 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]. Dataskyddsstyrelsen hyser därför farhågor över kommissionens fynd i förslaget till beslut om adekvat skyddsnivå vad gäller just denna typ av överföringar. Registrerade har vanligtvis ingen kännedom om ramen för uppgiftsskydd i tredjeländer. Det går därför inte att dra den slutsatsen att en registrerad kan bedöma risken med en överföring enbart genom att känna till det specifika destinationslandet. Tydlig information måste snarare ges om de specifika riskerna vid en sådan överföring av personuppgifter till ett land utanför Republiken Koreas territorium innan den registrerade ger sitt samtycke.

106. Dataskyddsstyrelsen uppmanar därför kommissionen att säkerställa att den information som ska lämnas till den registrerade ”om omständigheterna kring uppgiftsöverföringen” innehåller information om de möjliga riskerna med överföringen, till följd av avsaknaden av adekvat skydd i tredjelandet och av lämpliga skyddsåtgärder. Detta är viktigt för att dataskyddsstyrelsen ska kunna bedöma huruvida samtyckeskraven är väsentligen likvärdiga med GDPR.

107. Med tanke på att samtycke måste vara frivilligt, informerat, specifikt och entydigt, skulle dataskyddsstyrelsen välkomna att garantier införs i beslutet om adekvat skyddsnivå om att personuppgifter inte kommer att överföras från sydkoreanska personuppgiftsansvariga till tredje part i ett tredjeland i någon situation där ett giltigt samtycke enligt GDPR inte kan lämnas, t.ex. på grund av en obalans i befogenheter.

108. För fall där den personuppgiftsansvarige kan lämna personuppgifter till en tredje part utomlands utan den registrerades samtycke – dvs. 1) om personuppgifterna lämnas inom ett tillämpningsområde som är rimligen relaterat till det ursprungliga ändamålet för insamling enligt artikel 17.4 i PIPA; och 2) om personuppgifterna kan lämnas till en tredje part i de undantagsfall som nämns i artikel 18.2 i PIPA –

[42] Skäl 88 i förslaget till beslut.
[43] Se föregående fotnot.
[44] Se föregående fotnot.
[45] Europeiska dataskyddsstyrelsens riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679, den 25 maj 2018, s. 8.
[46] Europeiska dataskyddsstyrelsens riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679, den 25 maj 2018, s. 7.

noterar dataskyddsstyrelsen de förtydliganden som har lämnats av PIPC i avsnitt 2 i meddelande nr 2021-1 (och välkomnar att den personuppgiftsansvarige baserad i Sydkorea och mottagaren utomlands ska förpliktas att säkerställa en skyddsnivå som är likvärdig med PIPA, också vad gäller de registrerades rättigheter, genom ett rättsligt bindande instrument [såsom ett avtal]).

3.1.12. Direkt marknadsföring

109. Enligt artiklarna 21.2 och 21.3 i GDPR och GDPR:s referensram för adekvat skyddsnivå har den registrerade alltid kostnadsfritt kunnat invända mot behandlingen av uppgifter för ändamål som hänför sig till profilering och direkt marknadsföring.

110. Vad gäller rätten till upphävande som anges i artikel 37 i PIPA medger dataskyddsstyrelsen att kommissionen finner att denna rättighet också gäller i de fall där uppgifter används för direkt marknadsföring[47]. Dataskyddsstyrelsen välkomnar dock ytterligare information och förtydliganden i förslaget till beslut om denna bedömning och, i synnerhet, om den praktiska tillämpningen av rätten till upphävande vid direkt marknadsföring (t.ex. hänvisningar till relevant rättspraxis, osv.). I detta sammanhang vill dataskyddsstyrelsen även betona att rätten att begära att en leverantör/användare av kreditupplysningar slutar kontakta honom/henne för ändamål som hänför sig till att införa eller förhandla om köpet av varor eller tjänster uttryckligen framförs i CIA (artikel 37.2).

111. Såsom kommissionen erkänner[48] kräver en sådan behandling enligt den sydkoreanska rättsliga ramen i allmänhet ett särskilt (ytterligare) samtycke från den registrerade (se artikel 15.1. 1, artikel 17.2. 1 i PIPA).

112. Då det inte kan uteslutas att personuppgifter som överförs från EES kan behandlas i Sydkorea för sådana ändamål, skulle dataskyddsstyrelsen även välkomna förtydliganden i beslutet om adekvat skyddsnivå avseende förekomsten av en registrerads rättighet att återkalla sitt samtycke[49] och om rätten att få sina personuppgifter raderade och inte längre behandlade i de fall där behandlingen baseras på samtycke (såsom vid behandling för marknadsföringsändamål) och den registrerade har återkallat det.

3.1.13. Automatiserat beslutsfattande och profilering

113. Såsom Europeiska kommissionen bekräftar i sitt förslag till beslut[50] finns det inga allmänna bestämmelser i PIPA och dess genomförandeförordning för beslut som påverkar den registrerade och som enbart grundar sig på den automatiserade behandlingen av personuppgifter. Enligt det sydkoreanska rättsliga systemet finns det dock en sådan rätt i CIA, som innehåller regler om automatiserade beslut (artikel 36.2), även om deras tillämpning verkar ligga utanför området för PIPC:s tillsyn (och, som sådant, utanför området för detta förslag till beslut – se avsnitt 2.3.2 ovan avseende området för förslaget till beslut).

114. Som Artikel 29-gruppen[51] redan övervägt i sitt yttrande 1/2016 om skölden för skydd av privatlivet och dataskyddsstyrelsen i sitt yttrande om beslutet om adekvat skyddsnivå avseende Japan[52], skulle

[47] Skäl 79 i förslaget till beslut.
[48] Se föregående fotnot.
[49] Se även punkt 67 ovan: Samtidigt som möjligheten att återkalla sitt samtycke tydligt anges i artikel 37.1 i CIA, nämns denna rättighet bara två gånger i PIPA för specifika omständigheter i artiklarna 27.1 2 och artikel 39.7.
[50] Se skäl 81 i förslaget till beslut.
[51] Denna grupp 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.
[52] Yttrande 28/2018 om Europeiska kommissionens förslag till genomförandebeslut om adekvat skydd av personuppgifter i Japan, antaget den 5 december 2018.

den ökande betydelsen av automatiserat beslutsfattande, profilering och AI tyda på att ett mer skyddande synsätt intas i detta avseende. Till skillnad från kommissionens argument[53], enligt vilket avsaknaden av specifika regler om automatiserat beslutsfattande i PIPA högst osannolikt påverkar skyddsnivån för personuppgifter som insamlats i EU (eftersom ett eventuellt beslut baserat på automatiserad behandling i normala fall fattas av den personuppgiftsansvarige i EU som står i ett direkt förhållande till den berörda registrerade), anser dataskyddsstyrelsen att det inte kan uteslutas att en personuppgiftsansvarig baserad i Sydkorea kan använda automatiserat beslutsfattande vid överföring av uppgifter enligt beslutet om adekvat skyddsnivå (t.ex. i samband med anställning, för bedömning av arbetsinsats, tillförlitlighet, uppförande, osv.).

115. Genom att utveckla nya tekniker kan företag lättare genomföra eller överväga att genomföra system för automatiserat beslutsfattande som kan leda till att enskilda personers ställning försvagas. När beslut som enbart fattas av dessa automatiserade system inverkar på enskilda personers rättsliga situation eller påverkar dem signifikant (t.ex. genom att enskilda personer svartlistas och därigenom fråntas sina rättigheter) är det av största vikt att tillräckliga skyddsåtgärder införs, såsom rätten att bli informerad om de specifika skälen bakom beslutet och den berörda logiken, för att korrigera felaktig eller ofullständig information och bestrida beslutet när det har antagits på felaktig faktisk grund[54].

116. I detta sammanhang hyser dataskyddsstyrelsen farhågor över bristen på rättsliga bestämmelser om automatiserat beslutsfattande i PIPA och uppmanar därför kommissionen att bemöta dessa farhågor och fortsätta övervaka utvecklingen av den sydkoreanska rättsliga ramen avseende detta.

3.1.14. Ansvarsskyldighet

117. Den sydkoreanska rättsliga ramen innehåller flera regler som ska säkerställa att de personuppgiftsansvariga inför lämpliga tekniska och organisatoriska åtgärder för att effektivt kunna uppfylla sina skyldigheter avseende uppgiftsskydd och för att kunna visa att de uppfyller dem, bland annat till den behöriga tillsynsmyndigheten. Dataskyddsstyrelsen välkomnar i synnerhet närvaron av regler för att anta en intern förvaltningsplan (artikel 29 i PIPA), skyldigheten att utföra en s.k. konsekvensbedömning avseende dataskydd (nedan kallat *PIA*) i fall där behandlingen innebär en högre risk för möjliga kränkningar av integriteten (artikel 33.1 i PIPA och artikel 35 i PIPA:s genomförandeförordning), regler om utbildning och tillsyn av personal (artikel 28 i PIPA) samt skyldighet att utse en integritetsansvarig (artikel 31 i PIPA sammantaget med artikel 32 i PIPA:s genomförandeförordning).

118. Dataskyddsstyrelsen delar kommissionens uppfattning om det väsentligen likvärdiga skydd de säkerställer – också där reglerna verkar avvika från dem som anges i GDPR, såsom avsaknaden av en bestämmelse som anger att den integritetsansvarige måste vara oberoende, där det dock tydligt slås fast att han/hon måste rapportera till den personuppgiftsansvariges förvaltning (artikel 31.4 i PIPA) och att han/hon inte omotiverat får förlora sin rätt efter att ha utfört dessa funktioner (artikel 31.5 i PIPA) – och vill föreslå att kommissionen under sin granskning av beslutet om adekvat skyddsnivå övervakar den faktiska tillämpningen av dessa bestämmelser för att bedöma om de är ändamålsenligt genomförda.

3.2. Förfarande- och verkställandemekanismer

119. Utifrån de kriterier som anges i GDPR:s referensram för adekvat skyddsnivå har dataskyddsstyrelsen analyserat följande aspekter av den sydkoreanska ramen för uppgiftsskydd enligt förslaget till beslut: förekomsten av en oberoende och ändamålsenligt fungerande tillsynsmyndighet, förekomsten av ett system som säkerställer en god nivå av efterlevnad och ett system med tillgång till lämpliga

[53] Skäl 81 i förslaget till beslut.
[54] WP 254, s. 7.

prövningsmekanismer som ger enskilda personer i ESS möjlighet att utöva sina rättigheter och begära prövning utan att mötas av omständliga hinder för administrativ och rättslig prövning.

120. Enligt kapitel VI i GDPR och kapitel 3 i GDPR:s referensram för adekvat skyddsnivå måste det finnas minst en oberoende tillsynsmyndighet som har till uppgift att övervaka, säkerställa, och genomdriva överensstämmelse med bestämmelser om uppgiftsskydd och integritetsbestämmelser i ett tredjeland för att säkerställa en EES-likvärdig nivå av skydd.

121. I detta sammanhang måste tredjelandets tillsynsmyndighet vara fullständigt oberoende och opartisk när den utför sina uppgifter och utövar sina befogenheter och ska härvid varken begära eller ta emot instruktioner. Dessutom ska tillsynsmyndigheten ha alla nödvändiga och tillgängliga befogenheter och uppdrag för att säkerställa överensstämmelse med rättigheterna till uppgiftsskydd och öka medvetenheten. Dessutom bör tillsynsmyndighetens personal och budget beaktas. Tillsynsmyndigheten ska även, på eget initiativ, kunna inleda förfaranden.

3.2.1. Oberoende behörig tillsynsmyndighet

122. I Republiken Korea är PIPC den oberoende myndighet som har ansvar för övervakning och kontroll av PIPA. PIPC består av en ordförande, en vice ordförande och sju kommissionärer. Ordföranden och vice ordföranden utses av presidenten efter rekommendation från premiärministern. Av kommissionärerna utses två efter rekommendation från ordföranden, två efter rekommendation från representanter för det politiska parti som presidenten tillhör och de tre återstående ledamöterna efter rekommendation från representanter för andra politiska partier (artikel 7.2 2 i PIPA). PIPC ska biträdas av ett sekretariat (artikel 7.13) och kan upprätta underkommissioner (bestående av tre kommissionärer) för hantering av mindre överträdelser och återkommande frågor (artikel 7.12 i PIPA).
123. I detta avseende medger dataskyddsstyrelsen att PIC, trots den nyligen genomförda omorganiseringen som i grunden förändrade dess funktion och befogenheter, har gjort stora insatser för att bygga upp den infrastruktur som behövs för att tillmötesgå genomförandet av PIPA och dess senaste ändringar. Bland dessa insatser kan nämnas inrättandet av PIPC:s regler, utarbetandet av riktlinjer för vägledning om PIPA:s tolkning, och upprättandet av en hjälptelefon för rådgivning åt företagare och enskilda personer om bestämmelser för uppgiftsskydd samt en medlartjänst för att hantera klagomål. Arbetsuppgifterna för PIPC innefattar att ge råd om lagar och förordningar i samband med uppgiftsskydd, ta fram policyer och riktlinjer om uppgiftsskydd, undersöka överträdelser av individuella rättigheter, hantera klagomål, medla i tvister, genomdriva överensstämmelse med PIPA, säkerställa utbildning och befordran på området för uppgiftsskydd, samt utbyta och samarbeta med tredjelands myndigheter för uppgiftsskydd[55].

124. Utnämningen och sammansättningen av PIPC anges i artikel 7.2 i PIPA. Även om PIPC ligger inom premiärministerns behörighet (och ordföranden och vice ordföranden utses av presidenten efter rekommendation från premiärministern), föreskriver den rättsliga ramen att kommissionärerna utför sina uppdrag på ett oberoende sätt, i enlighet med lagen och med sina samveten. Dataskyddsstyrelsen bekräftar de institutionella och förfarandemässiga skyddsåtgärderna i PIPA och i synnerhet i artiklarna 7.4–7.7. Ändå skulle dataskyddsstyrelsen välkomna om kommissionen kunde övervaka all eventuell utveckling som kunde påverka ledamöternas oberoende i den sydkoreanska tillsynsmyndigheten.

125. Vidare innehåller förslaget till beslut ännu ingen analys av PIPC:s budget, inräknat finansieringskällor och budgetinsyn. Dataskyddsstyrelsen finner att denna ingående del, som nämns i både artikel 56.1 i GDPR och de förfarande- och verkställandeprinciper och -mekanismer för uppgiftsskydd som enligt GDPR:s referensram för adekvat skyddsnivå ska övervägas när ett lands eller en internationell organisations system utvärderas, måste noga beaktas eftersom den är en indikator på de ekonomiska och mänskliga resurser som tillsynsmyndigheten har tillgång till när den oberoende utför sina

[55] PIPC:s arbetsuppgifter och befogenheter anges främst i artiklarna 7.8 och 7.9, samt i artiklarna 61–66 i PIPA.

lagstadgade skyldigheter och uppgifter avseende uppgiftsskydd, och vill därför ge kommissionen rådet att närmare redovisa den i förslaget till beslut.

3.2.2. Förekomst av ett system för skydd av personuppgifter som säkerställer en god nivå av överensstämmelse

126. På området verkställande bekräftar dataskyddsstyrelsen den stora vidden av PIPC:s verkställande befogenheter och sanktioner enligt PIPA och CIA och noterar de förtydliganden som ingår meddelande nr 2021-1 enligt vilka de villkor som nämns i artikel 64.1 i PIPA och artikel 45.4 i CIA[56] kommer att äga giltighet närhelst någon av de principer, rättigheter och skyldigheter som ingår i lagen till skydd för personuppgifter överträds. Den skulle dock rekommendera kommissionen att noga övervaka den praktiska tillämpningen av PIPC:s befogenheter att förplikta lagöverträdaren att vidta de åtgärder den anser lämpliga enligt de som förtecknas i artikel 64.1 eller artikel 45.4 i CIA.

127. Vad gäller de korrigerande åtgärder som avses i artikel 64.1 i PIPA är PIPC, vid underlåtelse att iaktta en korrigerande åtgärd, bemyndigad att ålägga böter med ett högsta belopp på 50 miljoner sydkoreanska won (artikel 75.2 13 i PIPA). Detta belopp motsvarar 36 564 euro. Dataskyddsstyrelsen finner och befarar att ett sådant begränsat beloppsintervall för ekonomiska sanktioner kanske inte har en lika stark avskräckande effekt på lagöverträdare som lagen avser för att tillse iakttagandet av reglerna om uppgiftsskydd, och inte verkar tillräckligt omfattande för att avskräcka, särskilt vid stora organisationer eller företag med betydande ekonomiska resurser.

128. Vad gäller att PIPC skulle kunna begära att chefen för en central administrativ byrå undersöker den personuppgiftsansvarige eller gemensamt undersöker överträdelser av PIPA och t.o.m. ålägger korrigerande åtgärder mot personuppgiftsansvariga inom deras jurisdiktion (artiklarna 63.4–5 i PIPA), noterar dataskyddsstyrelsen att den övergripande karaktären av dessa andra byråer och deras rättsliga relationer till PIPC förblir tämligen oklara, trots att viss information har lämnats i skäl 122 i förslaget till beslut. Dessutom hänvisar artikel 681 i PIPA till många enheter som PIPC:s bemyndigande skulle kunna delegeras till. Även om denna bestämmelse bara verkar har tillämpats i förhållande till den sydkoreanska byrån för internet- och informationssäkerhet[57] skulle dataskyddsstyrelsen välkomna förtydliganden av typen av de möjliga interaktionerna mellan dessa enheter och att tillämpningen av denna bestämmelse noga övervakas i framtiden för att säkra oberoendet för de enheter som har ansvar för att tillämpa reglerna om uppgiftsskydd.

129. Vad gäller sanktioner verkar det sydkoreanska systemet kombinera olika typer av sanktioner, från korrigerande åtgärder och straffavgifter till straffrättsliga påföljder, vilka sannolikt har en stark avskräckande effekt. De sydkoreanska myndigheterna presenterade även flera exempel på avgifter som nyligen ålagts av PIPC, bland annat på 6,7 miljarder sydkoreanska won utfärdad i december 2020 till ett företag för att ha överträtt olika bestämmelser i PIPA, och en annan på 103,3 miljoner sydkoreanska won den 28 april 2021 utfärdad till ett AI-teknikföretag för att ha överträtt reglerna för laglig behandling av personuppgifter, i synnerhet samtycke, och behandlingen av pseudonymiserade uppgifter.

130. Även om de ovanstående beloppen kan ha en avskräckande effekt skulle dataskyddsstyrelsen välkomna mer information om den metod PIPC använder vid beräkningen av straffavgifternas nivå, till exempel för avgifter som åläggs för en underlåtelse att iaktta en korrigerande åtgärd som utfärdas i enlighet med artikel 64.1 i PIPA (se artikel 75.2 13 i PIPA). Detta är av särskild relevans för straffrättsliga påföljder och tillämpningen av (den sydkoreanska) brottslagstiftningen.

[56] Dvs. ”en överträdelse av lagen anses kunna inkräkta på enskilda personers rättigheter och friheter vad gäller personuppgifter och underlåtelse att vidta åtgärder kan orsaka skada som är svår att avhjälpa”.
[57] Se skäl 117 i förslaget till beslut och artikel 62 i genomförandeförordningen.

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

131. Vad gäller prövning verkar det sydkoreanska systemet erbjuda många olika former för att säkerställa ett adekvat skydd och, i synnerhet, verkställandet av individuella rättigheter med en ändamålsenlig administrativ och rättslig prövning, inräknat ersättning för skador.

132. Det sydkoreanska systemet erbjuder även alternativa mekanismer som enskilda personer kan vända sig till för att få rättelse, utöver administrativa och rättsliga former, såsom förklaras i skälen 132 och 133 i förslaget till beslut, avseende Privacy Call Centre respektive Dispute Mediation Committee. Eftersom dessa är ytterligare prövningsformer skulle dataskyddsstyrelsen välkomna utförligare förklaringar om hur de kompletterar möjligheterna till prövning inför PIPC och domstolarna för registrerade vars personuppgifter överförs till Sydkorea enligt beslutet om adekvat skyddsnivå.

4. TILLGÅNG TILL OCH ANVÄNDNING AV PERSONUPPGIFTER SOM ÖVERFÖRTS FRÅN EU AV OFFENTLIGA MYNDIGHETER I SYDKOREA

133. Vad gäller bedömningen av nivån av uppgiftsskydd inom områdena för brottsbekämpning och nationell säkerhet har Europeiska kommissionen lämnat utförlig information i sitt förslag till beslut och de tillgängliggjorda bilagorna. Dataskyddsstyrelsen avstår därför från att upprepa de flesta av de faktiska fynden och bedömningarna i detta yttrande.

134. Europeiska kommissionen drar slutsatsen att de områden som nämns ovan har en nivå av uppgiftsskydd som motsvarar kraven i EU-domstolens rättspraxis och som därför kan anses vara väsentligen likvärdig med den i EU.

135. Som allmän kommentar vill dataskyddsstyrelsen betona att också i fall där det verkar, eller kommissionen hävdar att det är, osannolikt att uppgifter som överförs från EU till Sydkorea berörs av den relevanta sydkoreanska lagstiftningen, är det i dessa fall ändå lämpligt att bedöma lämpligheten av den sydkoreanska nivån av uppgiftsskydd. Deras relevans framgår av det faktumet att Europeiska kommissionen själv har tagit upp dem i förslaget till beslut.

4.1. Allmän ram för uppgiftsskydd i samband med statlig tillgång

136. När det gäller offentliga myndigheters tillgång till personuppgifter måste många olika sydkoreanska lagar undersökas för att bedöma skyddsnivån för rätten till personlig integritet och uppgiftsskydd. För det första noterar dataskyddsstyrelsen att PIPA, i egenskap av central dataskyddslag, kräver bred tillämpning. Men medan PIPA är fullständigt tillämplig på brottsbekämpningsområdet, har den begränsad tillämpning på behandling av uppgifter för ändamål som hänför sig till nationell säkerhet. Enligt artikel 58.1 2 i PIPA, gäller inte kapitlen III–VII för behandling av personuppgifter för ändamål som hänför sig till nationell säkerhet. Trots detta förblir kapitlen I, II, IX och X tillämpliga för området nationell säkerhet. Både PIPA:s centrala principer och de grundläggande garantierna för registrerades rättigheter och bestämmelserna om tillsyn, verkställande och rättsmedel gäller därmed för nationella säkerhetsmyndigheters tillgång till och användning av personuppgifter.

137. Också i den sydkoreanska författningen fastställs väsentliga dataskyddsprinciper, nämligen principerna om laglighet, nödvändighet och proportionalitet. Dessa principer är också tillämpliga på de sydkoreanska offentliga myndigheternas tillgång till personuppgifter inom områdena för brottsbekämpning och nationell säkerhet[58].

[58] Se skäl 145 i förslaget till beslut.

138. På brottsbekämpningsområdet kan polis, åklagare, domstolar och andra offentliga organ samla in personuppgifter baserat på särskild lagstiftning, dvs. Criminal Procedure Act (nedan kallat *CPA*), Communications Privacy Protection Act (nedan kallat *CCPA*), Telecommunications Business Act (nedan kallat *TBA*) samt Act on Reporting and Using Specified Financial Transaction Information (nedan kallat *ARUSFTI*), som gäller för bekämpning och förebyggande av penningtvätt och finansiering av terrorism. I dessa särskilda lagar fastställs ytterligare begränsningar, skyddsåtgärder och undantag.

139. På området för nationell säkerhet kan den nationella underrättelsetjänsten (nedan kallat *NIS*), baserat på National Intelligence Service Act (nedan kallat *NISA*) och ytterligare ”nationella säkerhetslagar”[59] samla in personuppgifter och avlyssna kommunikationer. När NIS utövar sina befogenheter förstår dataskyddsstyrelsen att den måste följa både de tidigare nämnda rättsliga bestämmelserna och PIPA.

140. Dataskyddsstyrelsen ber kommissionen att klargöra huruvida det finns andra myndigheter i Sydkorea utöver NIS som ansvarar för området nationell säkerhet, eftersom kommissionen i bilaga I, avsnitt 6 ger intryck av att NIS är ett exempel på nationella säkerhetsbyråer.

4.2. Skydd och skyddsåtgärder för kommunikationsbekräftande data i samband med statlig tillgång för ändamål som hänför sig till brottsbekämpning

141. På grundval av den relevanta lagstiftningen, CPPA, kan brottsbekämpande myndigheter vidta två typer av åtgärder för att tillgå kommunikationsinformation. CPPA särskiljer mellan kommunikationsbegränsande åtgärder, som både täcker insamling av innehållet i vanlig post och direkt avlyssning av innehållet i telekommunikationer[60], och insamling av s.k. kommunikationsbekräftande data. I det senare ingår datumet för telekommunikationerna, deras start- och sluttidpunkt, antal utgående och inkommande samtal samt den andra partens abonnentnummer, användningsfrekvens, logfiler om användning av telekommunikationstjänster och information om varifrån samtalet kommer[61].

142. Dataskyddsstyrelsen noterar att kommunikationsbekräftande data inte verkar behöva omfattas av samma skyddsåtgärder som data som insamlas genom kommunikationsbegränsande åtgärder, dvs. innehållsdata. Faktum är att dataskyddsstyrelsen noterar att det behövs fler skyddsåtgärder vid insamlingen av innehåll än vid insamlingen av kommunikationsbekräftande data för ändamål som hänför sig till brottsbekämpning: För det första begränsas inte insamlingen av kommunikationsbekräftande data till undersökningen av vissa allvarliga brott, till skillnad från insamlingen av innehållsdata, utan kan utföras när så anses nödvändigt för att utföra ”en undersökning eller verkställa en bestraffning” (artikel 13.1 i CPPA). För det andra är insamlingen av kommunikationsbekräftande data i princip inte utformad som en sista utväg som bara används när det är svårt att på annat sätt förhindra att brott begås, gripa en brottsling eller samla in bevis[62]. Kommunikationsbekräftande data kan samlas in närhelst en åklagare eller polistjänsteman ”anser det nödvändigt” för att undersöka ett brott eller verkställa en bestraffning. Dock finns det i detta hänseende ett undantag för realtidsspårning av data och kommunikationsbekräftande data avseende en specifik basstation enligt artikel 13.2 i CPPA. För det tredje måste brottsbekämpande organ som samlar in innehållet i en kommunikation omedelbart avbryta denna aktivitet efter att det inte längre anses nödvändigt att ha fortsatt tillgång[63]. Vad gäller kommunikationsbekräftande data föreskrivs detta åtminstone inte uttryckligen i CPPA eller dess genomförandeförordning.

[59] I de nationella säkerhetslagarna ingår t.ex. Communications Privacy Protection Act, Act on Anti-Terrorism for the Protection of Citizens and Public Security, eller Telecommunications Business Act.
[60] Artiklarna 3.2, 2.6, 2.7 i CPPA.
[61] Artikel 2.11 i CPPA.
[62] Detta är fallet för innehållsdata enligt artikel 3.2 och 5.1 i CPPA.
[63] Artikel 2 i CPPA:s genomförandeförordning.

143. Dataskyddsstyrelsen noterar att insamling av kommunikationsbekräftande data endast får ske på grundval av domstolsbeslut. Vidare kräver CPPA tillhandahållandet av utförlig information både i ansökan om beslutet och i själva beslutet[64]. Ett sådant föregående domstolsgodkännande tjänar till att begränsa de brottsbekämpande myndigheternas utrymme för skönsmässig bedömning vid tillämpningen av lagen och att kontrollera om det i varje enskilt fall finns tillräckliga skäl för att samla in kommunikationsbekräftande uppgifter. Dataskyddsstyrelsen påpekar även att Republiken Koreas lagstiftning inte verkar ålägga en allmän och odifferentierad skyldighet att lagra kommunikationsbekräftande uppgifter. Statlig tillgång till sådana uppgifter avser därför alltid uppgifter som fortsätter att lagras för ändamål som hänför sig till fakturering och tillhandahållande av själva kommunikationstjänsterna.

144. Dataskyddsstyrelsen understryker dock att EU-domstolen har ifrågasatt att trafikdata är mindre känsligt än andra data, och särskilt mindre känsligt än innehållsdata[65]. Med tanke på att kommunikationsbekräftande data i flera hänseenden ges en lägre skyddsnivå än innehållsdata uppmanar dataskyddsstyrelsen kommissionen att noga övervaka huruvida skyddsåtgärder som föreskrivs enligt sydkoreansk lag för en sådan kategori av personuppgifter säkerställer en väsentligen likvärdig skyddsnivå med den som garanteras i EU, särskilt avseende lagens proportionalitet och förutsebarhet.

4.3. Sydkoreanska offentliga myndigheternas tillgång till kommunikationsinformation för ändamål som hänför sig till nationell säkerhet

145. Vad gäller den rättsliga ramen för nationella säkerhetsmyndigheters tillgång till kommunikationsinformation som överförs från EES till Sydkorea har dataskyddsstyrelsen identifierat två orosmoment, båda avseende en ordning för tillgång till kommunikationer mellan icke-koreanska medborgare som ingår i en särskild uppsättning användningsfall (se punkt 29). För både kommunikationsbekräftande data och innehållsdata gäller i dessa fall inte vissa skyddsåtgärder som annars föreskrivs. I dessa specifika fall drar dessa data med andra ord inte fördel av samma skyddsåtgärder som överförda data när minst en sydkoreansk medborgare är inblandad i kommunikationen.

4.3.1. Ingen skyldighet att meddela enskilda personer om statlig tillgång till kommunikationer mellan utländska medborgare

146. I ett scenario som det ovan, dvs. när ingen av parterna i en kommunikation är sydkoreansk medborgare, måste inte nationella säkerhetsmyndigheter meddela enskilda personer om insamlingen och behandlingen av deras personuppgifter. Dataskyddsstyrelsen inser att detta problem bara påverkar vissa fall. För det första, som redan har påpekats, närhelst minst en sydkoreansk medborgare är inblandad i kommunikationen gäller meddelandekraven enligt CPPA alla parter i kommunikationen oavsett deras medborgarskap[66]. För det andra omfattas insamlingen av personuppgifter som härrör

[64] Se skäl 156 i förslaget till beslut.

[65] Se EU-domstolen, C-623/17, *Privacy International*, den 6 oktober 2020, ECLI:EU:C:2020:790, punkt 71: ”Det ingrepp som överföring av trafik- och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna utgör i den rätt som är stadfäst i artikel 7 i stadgan måste betraktas som synnerligen allvarligt, bland annat med hänsyn till att den information som dessa uppgifter kan innehålla är känslig och i synnerhet till att det utifrån uppgifterna är möjligt att kartlägga de berörda personerna, då sådan information är lika känslig som själva innehållet i kommunikationerna. Det kan dessutom ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning (se, analogt, dom av den 8 april 2014, *Digital Rights Ireland m.fl.*, C‑293/12 och C‑594/12, EU:C:2014:238, punkterna 27 och 37, och dom av den 21 december 2016, *Tele2*, C‑203/15 och C‑698/15, EU:C:2016:970, punkterna 99 och 100).”

[66] Se skäl 192 i förslaget till beslut.

från kommunikationer som uteslutande sker mellan utländska medborgare av en särskild uppsättning användningsfall. I synnerhet omfattar rätten till tillgång i sådana fall kommunikationer av a) länder som är fientliga till Republiken Korea, b) utländska organ, grupper eller medborgare som misstänks för att delta i antikoreansk verksamhet[67], eller c) medlemmar i grupper som opererar inom Koreahalvön men i praktiken bortom Republiken Koreas suveränitet och deras paraplygrupper baserade i andra länder. Kommunikationer mellan enskilda personer i EU som överförs från EES till Sydkorea kan därmed samlas in för ändamål som hänför sig till nationell säkerhet om de omfattas av en av de tre kategorierna ovan[68]. Som ännu en begränsande faktor förstod dataskyddsstyrelsen av kommissionens närmare förklaringar att den tillämpliga rättsliga ramen inte föreskriver avlyssning av data vid överföring utanför Sydkorea.

147. Den kritiska betydelsen av bristen på ett meddelandekrav skulle därför anses vara begränsad vad gäller dess praktiska effekter. Dataskyddsstyrelsen understryker dock betydelsen av det (efterföljande) meddelandet om statlig tillgång, särskilt för att säkerställa effektiva rättsmedel. Enligt EU-domstolen är underrättelse ”nödvändig för att dessa personer ska kunna utöva sina rättigheter enligt artiklarna 7 och 8 i stadgan att begära tillgång till de av deras personuppgifter som är föremål för dessa åtgärder och, i förekommande fall, få dem rättade eller raderade, samt att i enlighet med artikel 47 första stycket i stadgan utöva sin rätt till ett effektivt rättsmedel inför en domstol”[69]. Statlig tillgång för ändamål som hänför sig till nationell säkerhet innefattar ofta hemliga övervakningsåtgärder, vilket innebär att de som står under övervakning, de registrerade, inte känner till behandlingen av deras personuppgifter. Det finns därför ”små möjligheter för den berörda personen att vända sig till domstol, såvida inte denne blir informerad om de åtgärder som vidtagits utan hans vetskap och på så sätt kan bestrida lagligheten för dessa retroaktivt [...] eller, som alternativ, såvida inte någon person som misstänker att hans kommunikation håller på att eller har avlyssnats kan vända sig till domstol så att domstolarnas domsrätt inte är avhängig något meddelande till den avlyssnade personen om att det har förekommit avlyssning av hans kommunikation”[70]. I detta sammanhang och i enlighet härmed har dataskyddsstyrelsen många gånger uttryckt sina farhågor över effektiva rättsmedel i övervakningsfall. Dataskyddsstyrelsen betonar att sekretessen i statliga åtgärder inte får leda till att sådana åtgärder i praktiken inte kan motsägas. Oavsett om bristen på ett meddelandekrav för kommunikationerna mellan utländska medborgare påverkar uppgiftsskyddets nivå såsom bedömts i bedömningen i förslaget till beslut, måste detta utvärderas som del av en helhetsbedömning, särskilt med tanke på mekanismerna för tillsyn och prövning som föreskrivs enligt sydkoreansk lag (se avsnitten 4.7 och 4.8).

148. Dessutom noterar dataskyddsstyrelsen i detta sammanhang att lagen hänvisar till tämligen breda termer såsom antikoreansk eller antinationell verksamhet[71] och att det är svårt att förstå hur dessa begrepp är konstruerade enligt sydkoreansk lag. Dataskyddsstyrelsen uppmanar kommissionen att övervaka hur dessa termer utarbetas i sydkoreansk lag och huruvida deras tillämpning i praktiken uppfyller kraven på proportionalitet i unionsrätten.

---

[67] Se bilaga II, fotnot 244, enligt vilken begreppet antikoreansk verksamhet avser aktiviteter som hotar nationens existens och säkerhet, demokratiska ordning eller människornas överlevnad och frihet.

[68] Se skäl 187 i förslaget till beslut.

[69] EU-domstolen, de förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.*, den 6 oktober 2020, ECLI:EU:C:2020:791, punkt 190.

[70] Europeiska domstolen för de mänskliga rättigheterna, *Big Brother Watch m.fl. mot Förenade kungariket*, den 25 maj 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punkt 337 och Europeiska domstolen för de mänskliga rättigheterna, målet *Roman Zakharov mot Ryssland*, den 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306, punkt 234.

[71] Europeiska kommissionen har förklarat att detta, enligt förklaringarna från den sydkoreanska regeringen, hänvisar till ”verksamhet som hotar nationens existens och säkerhet, demokratiska ordning eller människornas överlevnad och frihet”, se även fotnot 319 i förslaget till beslut om adekvat skyddsnivå.

4.3.2. Inget föregående oberoende godkännande för insamling av kommunikationsinformation mellan utländska medborgare

149. I de fall där EES-personuppgifter som härrör från kommunikationer mellan icke-koreanska medborgare (och som omfattas av ett av användningsfallen ovan) ska behandlas i Sydkorea för ändamål som hänför sig till nationell säkerhet, är insamlingen av dessa data inte underkastad föregående godkännande av ett oberoende organ (som är fallet för kommunikationer där minst en av de berörda individerna är sydkoreansk medborgare).[72]

150. Särskilt mot bakgrund av det aktuella domslutet från Europeiska domstolen för de mänskliga rättigheterna, *Big Brother Watch m.fl. mot Förenade kungariket* och *Centrum för Rättvisa mot Sverige*, finner dataskyddsstyrelsen det nödvändigt att utforska huruvida detta utgör ett allvarligt fel i den sydkoreanska ramen för uppgiftsskydd. Såsom betonas i dess uppdaterade rekommendationer om de europeiska nödvändiga garantierna för övervakningsåtgärder[73] erinrar dataskyddsstyrelsen i detta sammanhang om att det i artikel 6.3 i fördraget om Europeiska unionen fastställs att de grundläggande rättigheter som erkänns i Europakonventionen utgör allmänna principer i unionsrätten medan den senare, som EU-domstolen erinrar om i sin rättspraxis, inte utgör, så länge som EU inte har godtagit den, ett rättsligt instrument som formellt har införlivats i unionsrätten[74]. Den skyddsnivå för grundläggande rättigheter som krävs enligt artikel 45 i den allmänna dataskyddsförordningen ska därför fastställas på grundval av bestämmelserna i den förordningen, mot bakgrund av de grundläggande rättigheter som erkänns i stadgan. Med detta sagt ska, enligt artikel 52.3 i stadgan, rättigheterna däri som motsvarar de rättigheter som säkerställs i Europakonventionen ha samma innebörd och räckvidd som de som fastställs i denna konvention. Rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna avseende rättigheter som också föreskrivs i stadgan måste följaktligen beaktas, som ett lägsta tröskelvärde av skydd för att tolka de motsvarande rättigheterna i stadgan, dvs. i den utsträckning som stadgan, enligt EU-domstolens tolkning, inte föreskriver en högre skyddsnivå[75].

151. Medan ett föregående (oberoende) godkännande av övervakningsåtgärder betraktas som en viktig skyddsåtgärd mot godtycklighet, noterar dataskyddsstyrelsen att ett sådant godkännande inte kan härledas från EU-domstolens rättspraxis som ett absolut krav för proportionaliteten av övervakningsåtgärder. Europeiska domstolen för de mänskliga rättigheterna har dock nu uttryckligen fastställt kravet på ett i förväg genomfört oberoende godkännande för massavlyssning[76]. Även om det inte anges uttryckligen i förslaget till beslut, förstår dataskyddsstyrelsen att Republiken Koreas rättsliga ram inte föreskriver massavlyssning utan endast riktad avlyssning av telekommunikation[77]. Europeiska kommissionen har bekräftat denna förståelse.

---

[72] Se skäl 190 i förslaget till beslut.

[73] Se dataskyddsstyrelsens Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder, punkterna 10 och 11.

[74] Se EU-domstolen, C-311/18, *Data Protection Commissioner mot Facebook Ireland Ltd. och Maximilian Schrems*, den 16 juli 2020, ECLI:EU:C:2020:559 (nedan kallat *Schrems II-målet)*, punkt 98.

[75] Se EU-domstolen, Förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.*, den 6 oktober, punkt 124.

[76] Se Europeiska domstolen för de mänskliga rättigheterna, *Big Brother Watch m.fl. mot Förenade kungariket*, den 25 maj 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punkt 351: ”Massavlyssning ska inledningsvis underkastas oberoende godkännande”, ”massavlyssning ska godkännas av ett oberoende organ; dvs. ett organ som är oberoende i förhållande till den verkställande makten”.

[77] Endast bilaga II, avsnitt 3.2 innehåller en uttrycklig förklaring för ändamål som hänför sig till nationell säkerhet när det anges att begränsningarna och skyddsåtgärderna ”säkerställer att insamlingen och behandlingen av information är begränsade till vad som är strikt nödvändigt för att uppnå ett legitimt syfte”. Detta utesluter all

152. Med detta sagt visar de ovan nämnda domsluten från Europeiska domstolen för de mänskliga rättigheterna, i linje med EU-domstolens rättspraxis[78] och tidigare rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna[79], återigen på betydelsen av omfattande tillsyn av oberoende tillsynsmyndigheter. Dataskyddsstyrelsen betonar att oberoende tillsyn under samtliga stadier av statlig tillgång för ändamål som hänför sig till brottsbekämpning och nationell säkerhet är en viktig skyddsåtgärd mot godtyckliga övervakningsåtgärder och därmed för bedömningen av en adekvat nivå av uppgiftsskyddet. Garantin för tillsynsmyndigheternas oberoende i den mening som avses i artikel 8.3 i stadgan är avsedd att säkerställa en effektiv och tillförlitlig övervakning av efterlevnad av reglerna om skydd av enskilda personer med avseende på behandlingen av personuppgifter. Detta gäller i synnerhet under omständigheter där den enskilde personen, på grund av den hemliga övervakningens karaktär, hindras från att väcka talan eller från att direkt delta i alla prövningsförfaranden innan eller under det att övervakningsåtgärden utfördes.

153. Bristen på föregående oberoende godkännande kan inte i sig anses vara ett allvarligt fel i den sydkoreanska lagstiftningen avseende bedömningen av en väsentligen likvärdig nivå av uppgiftsskydd. Bedömningen av en adekvat skyddsnivå beror återigen på samtliga omständigheter i målet, särskilt på ändamålsenligheten av ex post tillsyn och rättslig prövning i enlighet med Sydkoreas rättsliga ram (se avsnitten 4.7 och 4.8).

4.4. Frivilliga utlämnanden av uppgifter

154. Enligt artikel 83.3 i TBA kan leverantörer av teletjänster frivilligt överlämna s.k. ”abonnentuppgifter”[80] till nationella säkerhetsmyndigheter och brottsbekämpande myndigheter på begäran. Dataskyddsstyrelsen noterar att fall av personuppgifter som överförts från EES till Sydkorea sannolikt är sällsynta men trots detta måste analyseras för att bedöma uppgiftsskyddets nivå, som redan nämnts ovan.

155. Dataskyddsstyrelsen förstår att PIPA:s skyddsåtgärder för dataskyddet gäller i dessa fall och att de offentliga myndigheterna, samt leverantörerna av teletjänster, måste uppfylla dessa krav[81] och att båda kan hållas ansvariga för alla kränkningar av de berörda registrerades rättigheter och friheter[82]. Vidare förstår dataskyddsstyrelsen att leverantörer av teletjänster inte är skyldiga att godta sådana framställningar.

156. Vad gäller begreppet tillgång till abonnentuppgifter av nationella brottsbekämpande myndigheter och i synnerhet för ändamål som hänför sig till nationell säkerhet genom "frivilligt utlämnande av uppgifter” om telekomoperatörer, befaras det dock att risken för de registrerades rättigheter och friheter ökar, särskilt vad gäller deras rätt till information.

157. Enligt artikel 58.1 2 i PIPA ska bestämmelserna i kapitlen III–VII inte gälla för personuppgifter som begärs tillhandahållas med avseende på nationell säkerhet. Bestämmelserna i till exempel artikel 18 (begränsning av användning och tillhandahållande av personuppgifter utanför ändamålet) och artikel 20 (meddelande om källor, osv. om personuppgifter som insamlas från tredje parter) i PIPA är

---

massinsamling och slumpartad insamling av personuppgifter för ändamål som hänför sig till nationell säkerhet ”.

[78] Se t.ex. EU-domstolen, de förenade målen C-203/15 och C-698/15, *Tele2 Sverige AB m.fl.*, ECLI:EU:C:2016:970.

[79] Se t.ex. Europeiska domstolen för de mänskliga rättigheterna, målet *Roman Zakharov mot Ryssland*, den 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Berörda dataset skulle vara: namn, nummer i folkbokföringsregistret, användarnas adress och telefonnummer, de datum då användarna tecknar eller avslutar sitt abonnemang samt användarnas identifieringskoder (används för att identifiera den rättmätige användaren av datorsystem eller kommunikationsnät).

[81] Se skälen 164 och 194 i förslaget till beslut.

[82] Se skäl 166 i förslaget till beslut.

i detta sammanhang inte tillämpliga på sådana framställningar. I de fall där en begäran görs av en nationell säkerhetsmyndighet väcker detta å ena sidan frågan huruvida artikel 58.1 2 även hindrar PIPA:s tillämpning på leverantörer av teletjänster. Å andra sidan uppstår frågan huruvida uteslutningen av tillämpningen av artikel 20 i PIPA i sådana fall också gäller den motsvarande bestämmelsen från avsnitt 3 i bilaga I (meddelande för de data där personuppgifter inte har erhållits från den registrerade [artikel 20 i lagen]). Om så inte var fallet och om artikel 58.1 2 också avsåg leverantörer av teletjänster skulle det enligt den tillgängliga informationen finnas en risk för att det inte skulle finnas någon rättslig förpliktelse att informera den registrerade om det frivilliga utlämnandet.

158. Dataskyddsstyrelsen befarar därför att informationskraven kan göras ineffektiva, så att de registrerade får det avsevärt svårare att hävda sin rätt till uppgiftsskydd, särskilt vad gäller rättsmedel. I detta sammanhang uppmanar dataskyddsstyrelsen kommissionen att förtydliga tillämpningsområdet för de relevanta bestämmelserna.

4.5. Ytterligare användning av information

159. Principen om ändamålsbegränsning är ett centralt rättsligt krav för uppgiftsskydd. Den innebär att personuppgifter bara får samlas in för specificerade, uttryckliga och legitima syften och inte ytterligare behandlas på ett sätt som är oförenligt med dessa syften. Vidare tillåter unionsrätten att offentliga myndigheter behandlar personuppgifter för att förebygga, utreda eller lagföra brott, också om dessa uppgifter inledningsvis erhölls för andra ändamål, om dessa myndigheter har en rättslig grund för att behandla dessa uppgifter enligt relevant lagstiftning och om den ytterligare behandlingen inte är oproportionerlig[83].

160. Enligt denna noterar dataskyddsstyrelsen att liknande skyddsåtgärder och begränsningar föreskrivs i den sydkoreanska ramen för uppgiftsskydd som de i unionsrätten för de ytterligare användningarna av den information som insamlats för ändamål som hänför sig till brottsbekämpning och nationell säkerhet, t.ex. artikel 3.1–2 i PIPA:s princip om ändamålsbegränsning.

4.6. Vidare överföringar och underrättelseutbyte

161. I artikel 44 i GDPR fastställs det att överföringar och vidare överföringar av personuppgifter endast får ske om den nivå på skyddet som säkerställs genom GDPR inte undergrävs. Skyddsnivån för personuppgifter som överförs från EES till Sydkorea får därför inte undergrävas av vidare överföringar till mottagare i ett tredjeland, dvs. vidare överföringar ska endast tillåtas när en fortsatt skyddsnivå är väsentligen likvärdig med den som säkerställs i unionsrätten. Vid bedömningen av huruvida ett tredjeland säkerställer en adekvat nivå av uppgiftsskydd måste följaktligen landets rättsliga ram för vidare överföringar beaktas. Detta är obestridligt och i linje med både Europeiska kommissionens[84] och dataskyddsstyrelsens uppfattning.

162. I detta sammanhang noterar dataskyddsstyrelsen att Europeiska domstolen för de mänskliga rättigheterna i sina aktuella domslut *Big Brother Watch m.fl. mot Förenade kungariket* och *Centrum för Rättvisa mot Sverige* har tillhandahållit vägledning[85] om de försiktighetsåtgärder för uppgiftsskydd som ska iakttas i avtalsslutande stater som tillhandahåller personuppgifter till andra parter för

[83] Se artikel 4.2 i LED.

[84] Se skäl 84 och följande i förslaget till beslut.

[85] Följande element fastställdes med anledning av fallen *Big Brother Watch* och *Centrum för Rättvisa*, som rör massavlyssningsregimer. Kravet på skyddsåtgärder som ska vidtas när material tillhandahålls till andra parter ingick redan i de kriterier som togs fram av Europeiska domstolen för de mänskliga rättigheterna i samband med riktad avlyssning och hade inte vidare specificerats av Europeiska domstolen för de mänskliga rättigheterna (se *Big Brother Watch m.fl. mot Förenade kungariket*, punkterna 335 och 362).

ändamål som hänför sig till brottsbekämpning och nationell säkerhet i massinsamlingsfall: ”För det första ska de omständigheter inom vilka en sådan överföring får ske vara tydligt fastställda i nationella lagstiftning. För det andra måste den överförande staten säkerställa att den mottagande staten har installerat skyddsåtgärder som förmår hindra missbruk och oproportionerliga ingrepp. I synnerhet måste den mottagande staten garantera en säker lagring av materialet och begränsa dess vidarebefordran. […] För det tredje kommer förhöjda skyddsåtgärder att behövas när det är tydligt att material som kräver särskild konfidentialitet – såsom konfidentiellt journalistiskt material – överförs.”[86]

163. När Europeiska domstolen för de mänskliga rättigheterna tillämpade dessa standarder fann den i ”Centrum för Rättvisa mot Sverige” att avsaknaden av alla uttryckliga rättsliga krav i avlyssningsregimen för att bedöma nödvändigheten och proportionaliteten av underrättelseutbyte vad gäller dess möjliga effekt på rätten till personlig integritet utgör en överträdelse av artikel 8 i Europakonventionen. Europeiska domstolen för de mänskliga rättigheterna kritiserade att den allmänna utformningen av lagen gjorde det i allmänhet möjligt att skicka avlyssnat material till utlandet närhelst så anses vara av nationellt intresse, oavsett om den utländska mottagaren erbjuder en godtagbar miniminivå av skyddsåtgärder eller inte[87].

164. Med hänsyn till att Sydkoreas rättsliga ram inte tillåter massavlyssning finner dataskyddsstyrelsen, fortfarande mot bakgrund av följderna av rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna såsom beskrivs ovan, utöver de krav som följer av unionsrätten enligt EU-domstolens tolkning, att de argument som framförs av Europeiska domstolen för de mänskliga rättigheterna bör övervägas för att bedöma huruvida adekvata standarder för uppgiftsskyddet föreskrivs i den rättsliga ramen för vidare överföringar till ett tredjeland.

4.6.1. Tillämplig rättslig ram för vidare överföringar av brottsbekämpande myndigheter

165. Vad gäller de behöriga myndigheternas vidare överföringar för ändamål som hänför sig till brottsbekämpning förstår dataskyddsstyrelsen av kommissionens förklaringar att avsnitt 2 i bilaga I till förslaget till beslut avseende begränsning av vidare överföringar ska tillämpas, bl.a. när överföringen görs på grundval av en annan stadga än PIPA. Enligt denna regel gäller följande: ”om personuppgifter tillhandahålls till en tredje part utomlands kan det hända att de inte omfattas av den skyddsnivå som garanteras av Sydkoreas Personal Information Protection Act, på grund av skillnader i olika länders system för skydd för personuppgifter. Sådana fall kommer därför att anses vara ”fall där olägenheter kan ha orsakats den registrerade” enligt stycke 4 i artikel 17 i lagen eller ”fall där en registrerads eller tredje parts intressen otillbörligt åsidosätts” enligt stycke 2 i artikel 18 i lagen och artikel 14.2 i genomförandeförordningen till samma lag. För att uppfylla kraven i dessa bestämmelser måste den personuppgiftsansvarige och tredje part därför uttryckligen säkerställa en skyddsnivå motsvarande lagen, inräknat garantin för den registrerades utövande av sina rättigheter i rättsligt bindande handlingar såsom kontrakt, också efter det att personuppgifter överförts till utlandet”[88].

166. Dataskyddsstyrelsen välkomnar denna bestämmelse, som, med antagande av en adekvat nivå av uppgiftsskydd i Sydkorea för detta ändamål, säkerställer kontinuiteten för en skyddsnivå som är väsentligen likvärdig med den som erbjuds enligt unionsrätten för vidare överföringar. Kommissionen har bekräftat att dataskyddsstyrelsens förståelse är korrekt, dvs. att detta avsnitt i bilaga I gäller för alla vidare överföringar för ändamål som hänför sig till brottsbekämpning. Dataskyddsstyrelsen påpekar dock att det måste säkerställas att det i denna förordning föreskrivs en i praktiken fortsatt skyddsnivå, då det kan råda osäkerhet om de avtalsmässiga skyddsåtgärder och skyldigheter eller

[86] Europeiska domstolen för de mänskliga rättigheterna, *Big Brother Watch m.fl. mot Förenade kungariket*, den 25 maj 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punkt 362

[87] Se Europeiska domstolen för de mänskliga rättigheterna, *Centrum för Rättvisa mot Sverige*, den 25 maj 2021, ECLI:CE:ECHR:2021:0525JUD003525208, punkt 326.

[88] Förslaget till beslut, bilaga I, s 7.

andra liknande mekanismer som kan användas för att uppnå en sådan skyddsnivå vid behandling för ändamål som hänför sig till brottsbekämpning. I detta sammanhang ska det till exempel dessutom anges att personuppgifter endast får utbytas med de relevanta behöriga myndigheterna i tredjelandet.

167. Under förutsättning av ett förtydligande, såsom begärs ovan, av huruvida KOFIU ingår i förslaget till beslut, noterar dataskyddsstyrelsen att det i den officiella representationen om statlig tillgång[89] förklaras att KOFIU:s kommissionär, enligt artikel 8.1 i ARUSFTI, kan förse andra länders underrättelsetjänster på finansområdet med specificerade uppgifter om finansiella transaktioner, om så anses nödvändigt för att uppnå ändamålet med ARUSFTI[90]. Artikel 8 i ARUSFTI föreskriver ingen skyldighet att bestämma huruvida, eller att säkerställa att, det andra landet erbjuder en adekvat skyddsnivå för uppgiftsskydd. Bilaga II hänvisar inte till det nya avsnittet i bilaga I i detta avseende. Dataskyddsstyrelsen uppmanar därför kommissionen att förtydliga det inbördes sambandet mellan det relevanta avsnittet i bilaga I om begränsning av vidare överföringar och den rättsliga grunden för vidare överföringar enligt ARUSFTI.

4.6.2. Tillämplig rättslig ram för vidare överföringar för ändamål som hänför sig till nationell säkerhet

168. Förslaget till beslut innehåller ingen information om den rättsliga ramen för vidare överföringar på området för nationell säkerhet. Dataskyddsstyrelsen förstår därav att avsnitt 2 i bilaga I inte är tillämpligt på vidare överföringar för ändamål som hänför sig till nationell säkerhet, till skillnad från ändamål som hänför sig till brottsbekämpning. Artiklarna 17 och 18 i PIPA i det berörda bilaga I-avsnittet ingår i kapitel III i PIPA, som i sin tur inte är tillämpligt på behandlingen av personuppgifter för ändamål som hänför sig till nationell säkerhet (artikel 58.1 i PIPA).

169. Dataskyddsstyrelsen antar dock att Sydkorea kan behöva överföra och faktiskt överför personuppgifter till utländska underrättelsetjänster för ändamål som hänför sig till nationell säkerhet, t.ex. för att samarbeta om att bekämpa gränsöverskridande hot mot den nationella säkerheten, varna utländska regeringar om dessa eller inhämta deras hjälp för att identifiera sådana hot.

170. Dataskyddsstyrelsen förstod att vidare överföringar enligt kommissionens uppfattning är tillräckligt reglerade i sydkoreansk lagstiftning genom de skyddsåtgärder som följer av den övergripande konstitutionella ramen, i synnerhet principerna om nödvändighet och proportionalitet, samt genom PIPA:s centrala principer om uppgiftsskydd, t.ex. laglig och korrekt behandling, ändamålsbegränsning, uppgiftsminimering, säkerhet och de allmänna skyldigheterna att förhindra missbruk och felaktig användning av personuppgifter.

171. Dataskyddsstyrelsen förstår och värdesätter den allmänna tillämpligheten av dessa centrala principer (om uppgiftsskydd), men finner det oroande att dessa skyddsåtgärder är mycket allmänt hållna och inte specifikt hänvisar till eller tar upp, på en rättslig grund, de specifika omständigheterna och villkoren för vidare överföringar av EES-överförda uppgifter för ändamål som hänför sig till nationell säkerhet. Då dessa allmänna och övergripande principer har bred tillämpning, ifrågasätter dataskyddsstyrelsen om detta skulle kunna anses uppfylla kraven på tydliga och precisa regler och om det tillräckligt befäster verkningsfulla och verkställbara skyddsåtgärder. Särskilt när statlig tillgång och behandling av personuppgifter utövas i hemlighet och de slutsatser som kan dras av dessa uppgifter

[89] Se förslaget till beslut, bilaga II.

[90] Se förslaget till beslut, bilaga II, avsnitt 2.2.3.2. Då ett sådant utbyte endast får ske förutsatt att den utländska tjänsten inte får använda informationen för något annat ändamål än det ursprungliga ändamålet för utlämnande, och särskilt inte för en brottsundersökning eller rättegång (artikel 8.2 i ARUSFTI), kan KOFIU:s kommissionär, efter att ha mottagit en utländsk begäran, samtycka till att sådana data används för brottsundersökningar eller brottmålsrättegångar med ett föregående samtycke från justitieministeriet (artikel 8.3 i ARUSFTI).

är särskilt allvarliga, är det viktigt att ha tydliga, detaljerade regler. Lagen bör tillräckligt klart reglera omfattningen av de behöriga myndigheternas befogenheter och det närmare utövandet av dem för att ge den enskilde personen tillräckligt skydd. I sin dom i *Schrems II*-målet erinrar EU-domstolen om att en rättslig grund som medger ingrepp i grundläggande rättigheter måste, för att uppfylla kraven i principerna om nödvändighet och proportionalitet, själv definiera tillämpningsområdet för begränsningen av utövandet av den berörda rättigheten samt fastställa tydliga och precisa regler för den berörda åtgärdens tillämpningsområde och tillämpning och införa en miniminivå av skyddsåtgärder[91]. Dataskyddsstyrelsen befarar därför att det inte är tillräckligt att sådana skyddsåtgärder allmänt erkänns i överordnade rättsregler utan att t.ex. begreppet proportionalitet samtidigt specifikt genomförs i den respektive rättsliga grunden i sig.

172. Dessa farhågor understöds av det ovan nämnda beslutet från Europeiska domstolen för de mänskliga rättigheterna, i vilket domstolen fann att en allmän regel utan något uttryckligt krav att bedöma nödvändighet och proportionalitet eller beakta farhågor för den personliga integriteten inte är förenlig med rätten till personlig integritet enligt artikel 8 i Europakonventionen. I samband med detta noterar dataskyddsstyrelsen att den berörda lagen (liksom den sydkoreanska lagen) faktiskt innehåller övergripande (konstitutionellt garanterade) principer om nödvändighet och proportionalitet, t.ex. i enlighet med stadgan och genom anslutningen till Europakonventionen.

173. Dataskyddsstyrelsen uppmanar kommissionen att förtydliga den rättsliga grunden, hur, i vilken omfattning och på vilka konkreta villkor underrättelsetjänster är tvungna att beakta farhågor över den personliga integriteten och skyddsåtgärder för dataskyddet, innan personuppgifter utlämnas till partner i andra länder för ändamål som hänför sig till nationell säkerhet. Om en sådan skyldighet härrör direkt ur konstitutionella principer bör kommissionen närmare bedöma kraven på precision och klarhet i den relevanta lagen och bekräfta att de allmänna konstitutionella och dataskyddsrelaterade principerna är korrekt tillämpade och genomförda.

4.6.3. Internationella avtal

174. Dataskyddsstyrelsen noterar att kommissionen, som del av sin bedömning av adekvat skyddsnivå, inte har beaktat de internationella avtal som har slutits mellan Republiken Korea och tredjeländer eller internationella organisationer, i vilka särskilda bestämmelser kan vara föreskrivna för internationell överföring av personuppgifter av brottsbekämpande myndigheter och/eller underrättelsetjänster till tredjeländer. Dataskyddsstyrelsen finner att slutandet av bilaterala eller multilaterala avtal med tredjeländer för ändamål som hänför sig till brottsbekämpnings- eller underrättelsesamarbete sannolikt påverkar Sydkoreas ram för uppgiftsskydd enligt bedömning.

175. Dataskyddsstyrelsen uppmanar kommissionen att klargöra om sådana avtal finns, på vilka villkor de kan ha slutits och bedöma om bestämmelserna i internationella avtal kan påverka skyddsnivån för personuppgifter som överförs från EES till Sydkorea genom den rättsliga ramen och praxis i förhållande till utlämnanden till utlandet för ändamål som hänför sig till brottsbekämpning och nationell säkerhet.

4.7. Tillsyn

176. Dataskyddsstyrelsen noterar att tillsynen över strafflagstiftningens genomförande liksom nationella säkerhetsmyndigheter garanteras av en kombination av olika interna och externa organ.

177. Det ska i detta sammanhang noteras att EU-domstolen vid upprepade tillfällen har betonat behovet av oberoende tillsyn som en avgörande komponent i skyddet av fysiska personer avseende behandlingen av deras personuppgifter. Begreppet oberoende täcker in områdena institutionell självständighet, frihet från instruktioner och materiellt oberoende. För att säkerställa en enhetlig

[91] Se *Schrems II*, punkterna 175 och 180.

övervakning och tillämpning av dataskyddslagen måste tillsynsmyndigheterna ha verkliga befogenheter, däribland korrigerande befogenheter.

178. Dataskyddsstyrelsen tillstyrker kommissionens slutsats om att Sydkorea kan, vid en helhetsbedömning, anses inneha ett oberoende och effektivt tillsynssystem även om flera organ i tillsynssystemet inte själva uppfyller ovanstående krav. De flesta av dem har till exempel inga genomförandebefogenheter, utan är begränsade till enbart rekommendationer, t.ex. National Human Rights Commission eller Board of Audits and Inspections. Vidare är de flesta av de respektive offentliga organen inte enbart institutioner för uppgiftsskydd, utan tilldelas oftast andra arbetsuppgifter inom andra områden av skyddet av de grundläggande rättigheterna.

179. Dataskyddsstyrelsen noterar dock att tillsynen av brottsbekämpande myndigheter, enligt kommissionens förklaringar, garanteras totalt och utan undantag av PIPC. Därför innehar PIPC undersökande, korrigerande och verkställande befogenheter enligt PIPA och andra dataskyddslagar (t.ex. CPPA), som gäller för hela området av brottsbekämpande myndigheters och nationella säkerhetsmyndigheters tillgång till personuppgifter.

180. I detta sammanhang vill dataskyddsstyrelsen återigen betona att tillsynsmyndigheter måste förses med tillräckliga mänskliga, tekniska och finansiella resurser för att kunna utöva sina uppgifter och befogenheter. För att uppnå detta saknas det tyvärr information om de utsedda tillsynsorganen, särskilt PIPC. Av denna anledning upprepar dataskyddsstyrelsen sin begäran till kommissionen att tillhandahålla ytterligare information om ärendet.

181. Totalt sett noterar dataskyddsstyrelsen att knappast några yttranden, exempel eller siffror förekommer i förslaget till beslut avseende tillsynsverksamheten eller tillsynsorganens rättsliga verkställande av dataskyddslagen på området för brottsbekämpning och nationell säkerhet. Dessa skulle vara värdefulla vid utvärderingen av tillsynsorganens ändamålsenlighet.

1.8. Rättsmedel och prövning

182. Dataskyddsstyrelsen erinrar dock om att det är avgörande för en adekvat nivå av uppgiftsskydd att de registrerade får tillgång till omfattande rättsmedel och domstolsprövning mot otillåten tillgång eller behandling av uppgifter. Dessa rättsmedel måste vara tillräckliga för att den registrerade ska kunna få tillgång till sina lagrade personuppgifter samt begära att de korrigeras eller raderas.

183. Mot bakgrund av EU-domstolens domar i målen *Schrems I* och *Schrems II* är det tydligt att, utöver rätten att kunna vända sig till behöriga myndigheter, ett effektivt rättsligt skydd i den mening som avses i artikel 47.1 i stadgan är av grundläggande betydelse för antagandet att ett tredjeland innehar en adekvat lagstiftning.

184. Dataskyddsstyrelsen inser att Sydkorea har fastställt olika former för verkställandet av individuella rättigheter till tillgång, lagring, radering och upphävande enligt PIPA. Dessa rättigheter kan verkställas gentemot den personuppgiftsansvarige själv eller via ett klagomål som lämnats in till PIPC eller andra tillsynsorgan, t.ex. National Human Rights Commission. Vidare inser dataskyddsstyrelsen möjligheten att överklaga personuppgiftsansvarigas eller offentliga myndigheters beslut som svar på deras begäran på grundval av förvaltningsprocesslagen.

185. Vidare förstår dataskyddsstyrelsen av kommissionens förklaringar att enskilda personer kan överklaga brottsbekämpande myndigheters och nationella säkerhetsmyndigheters åtgärder vid behöriga domstolar enligt förvaltningsprocesslagen och författningsdomstolslagen, och har möjlighet att erhålla ersättning för skador enligt lagen om statlig ersättning[92].

[92] Se bilaga II, 3.2.4 sammantaget med 2.4.3.

186. I detta sammanhang hyser dock dataskyddsstyrelsen farhågor över den effektiva prövningen för enskilda personer i EU i nationella säkerhetsfall där ingen sydkoreansk medborgare är involverad. Såsom påpekas i stycke 33 och följande är nationella säkerhetsmyndigheter inte ålagda att meddela registrerade om insamlingen och behandlingen av deras personuppgifter. Eftersom det är avsevärt svårare att i dessa fall erhålla effektivt juridiskt skydd, vill dataskyddsstyrelsen påpeka att det här krävs vissa juridiska skyddsåtgärder om det rör sig om uppgifter som överförts från EES. Dessa skyddsåtgärder måste göra det möjligt för de registrerade att vidta verkningsfulla åtgärder mot otillåten uppgiftsbehandling på ett juridiskt säkert sätt utan att hindras av överdrivet smala förfarandekrav, t.ex. genom införandet av en bevisbörda som de inte kan uppfylla utan vetskap om behandlingen. Vidare måste de registrerade kunna vända sig till ett behörigt organ som uppfyller kraven i artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna, dvs. som är behörigt att avgöra att en uppgiftsbehandling föreligger, liksom kontrollera behandlingens laglighet, och som har effektiva korrigerande befogenheter ifall uppgiftsbehandlingen är olaglig. Mot denna bakgrund skulle enbart en rätt att klaga exempelvis vid NHRC inte vara tillräckligt. Dataskyddsstyrelsen uppmanar därför kommissionen att närmare förklara hur dessa krav genomförs vad gäller förfarandet och i sak, t.ex. om det är möjligt för registrerade att både vända sig till PIPC och till en domstol utan att vara tvungna att bevisa den berörda uppgiftsbehandlingen.

187. Dessutom noterar dataskyddsstyrelsen att det i förslaget till beslut föreskrivs en mekanism för hänskjutande av klagomål, dvs. att enskilda personer i EU kan lämna in ett klagomål till PIPC genom sin nationella myndighet för uppgiftsskydd eller dataskyddsstyrelsen. PIPC kommer därefter att meddela den enskilde personen genom samma kanaler efter avslutad undersökning[93]. Dataskyddsstyrelsen välkomnar ansträngningarna att underlätta tillgången till prövning mot sydkoreanska nationella säkerhetsmyndigheter. Samtidigt förespråkar dataskyddsstyrelsen att denna prövningsmekanism förmedlas genom europeiska nationella myndigheter för uppgiftsskydd snarare än genom dataskyddsstyrelsen, eftersom de är behöriga och befinner sig närmare hanteringen av enskilda klagomål.

188. Vidare noterar dataskyddsstyrelsen en eventuell konflikt med frivilliga utlämnanden av uppgifter. Å ena sidan hävdas det i förslaget till beslut att enskilda personer ska kunna få rättslig prövning om deras personuppgifter utlämnas olagligen efter en begäran om ett frivilligt utlämnande av uppgifter, däribland mot den brottsbekämpande myndighet som utfärdar begäran[94]. Å andra sidan tas det i förslaget till beslut upp kravet på direkt påverkan vad gäller den enskildes rätt att överklaga offentliga myndigheters åtgärder, där (endast) bindande framställningar om utlämnande listas som exempel på ett fall där en administrativ åtgärd anses direkt påverka rätten till personlig integritet[95]. Dataskyddsstyrelsen förstår av kommissionens förklaringar att möjligheterna till prövning mot framställningar om frivilligt utlämnande faktiskt saknar begränsning och ber därför kommissionen att närmare förtydliga detta i beslutet, både på området för brottsbekämpning och för nationell säkerhet (till skillnad från avsnittet om brottsbekämpning innehåller avsnittet om frivilligt utlämnande för ändamål som hänför sig till nationell säkerhet inget direkt yttrande om prövning i detta sammanhang).

[93] Se skäl 205 och bilaga 1, s. 19 i förslaget till beslut.
[94] Se skäl 166 i förslaget till beslut.
[95] Se skäl 181 (brottsbekämpning) och skälen 208 och 181 (nationell säkerhet) i förslaget till beslut.