Udtalelse 32/2021 om Europa-Kommissionens udkast til gennemførelsesafgørelse i henhold til forordning (EU) 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Republikken Korea

Version 1.0

Vedtaget den 24. september 2021

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

INDHOLD

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 70, stk. 1, litra s), i Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF ("**GDPR**"),

under henvisning til aftalen om Det Europæiske Økonomiske Samarbejdsområde ("**EØS**"), særlig bilag XI og protokol 37 til EØS-aftalen, ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018[1],

under henvisning til artikel 12 og artikel 22 i forretningsordenen,

— VEDTAGET FØLGENDE UDTALELSE:

1. RESUMÉ

1. Europa-Kommissionen indledte den 16. juni 2021[2] den formelle proces hen imod vedtagelse af sit udkast til gennemførelsesafgørelse ("**udkast til afgørelse**") om tilstrækkelig beskyttelse af personoplysninger i Republikken Korea i henhold til loven om beskyttelse af personoplysninger i medfør af GDPR.

2. Samme dag anmodede Europa-Kommissionen Det Europæiske Databeskyttelsesråd ("**Databeskyttelsesrådet**") om en udtalelse[3]. Databeskyttelsesrådets vurdering af, om beskyttelsesniveauet i Republikken Korea er tilstrækkeligt, er foretaget på grundlag af gennemgangen af selve udkastet til afgørelse samt på grundlag af en analyse af den dokumentation, som Europa-Kommissionen har stillet til rådighed[4].

3. Databeskyttelsesrådet fokuserede på vurderingen af både de generelle GDPR-aspekter ved udkastet til afgørelse og offentlige myndigheders indsigt i personoplysninger, der overføres fra EØS med henblik på retshåndhævelse og national sikkerhed, herunder hvilke retsmidler der er til rådighed for borgere i EØS. Databeskyttelsesrådet vurderede også, om garantierne i Koreas retlige ramme er indført og er effektive.

4. Databeskyttelsesrådet har som hovedreference for dette arbejde anvendt sin reference vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR[5] ("**reference vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR**"), der blev vedtaget i februar 2018, og Databeskyttelsesrådets anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger[6].

[1] Henvisninger til "**medlemsstater**" i denne udtalelse skal forstås som henvisninger til "EØS-medlemsstater".
[2] Se pressemeddelelse https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Ibid.
[4] Databeskyttelsesrådet baserede sin analyse på officielle oversættelser udarbejdet af den koreanske regering.
[5] WP254, reference vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR, 6. februar 2018, (godkendt af Databeskyttelsesrådet, jf. https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Jf. Databeskyttelsesrådets anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, der blev vedtaget den 10. november 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

1.1. Områder med konvergens

5. Databeskyttelsesrådets hovedmål er at afgive en udtalelse til Europa-Kommissionen om, hvorvidt beskyttelsesniveauet for fysiske personer, hvis personoplysninger overføres til Republikken Korea, er tilstrækkeligt. Det er vigtigt at fastslå, at Databeskyttelsesrådet ikke forventer, at Koreas ramme for databeskyttelse er en kopi af den europæiske lovgivning om databeskyttelse.

6. Databeskyttelsesrådet minder imidlertid om, at for at tredjelandets lovgivning kan anses for at sikre et tilstrækkeligt beskyttelsesniveau, kræver artikel 45 i GDPR samt retspraksis ved Den Europæiske Unions Domstol ("**Domstolen**"), at den tilpasses kernen i de grundlæggende principper i GDPR. I den forbindelse har Koreas ramme for databeskyttelse mange ligheder med den europæiske ramme for databeskyttelse, idet den indeholder én primær retsakt, der dækker både den offentlige og den private sektor, og som suppleres af sektorspecifikke retsakter.

7. Hvad angår indholdet, bemærker Databeskyttelsesrådet centrale områder for tilpasning mellem GDPR-rammen og Koreas ramme for databeskyttelse med hensyn til visse centrale bestemmelser, såsom begreber (f.eks. "personoplysninger", "behandling" og "den registrerede"); grunde til lovlig og rimelig behandling til legitime formål; formålsbegrænsning; datakvalitet og proportionalitet; dataopbevaring; sikkerhed og fortrolighed; gennemsigtighed; og særlige kategorier af oplysninger.

8. Ud over ovenstående bifalder Databeskyttelsesrådet den indsats, som Europa-Kommissionen og de koreanske myndigheder har gjort for at sikre, at Republikken Korea sikrer et tilstrækkeligt beskyttelsesniveau i forhold til GDPR gennem den koreanske tilsynsmyndigheds vedtagelse af underretninger (ikke kun gældende for personoplysninger, der overføres fra EØS til Korea) med henblik på at udfylde hullerne mellem GDPR og Koreas ramme for databeskyttelse. I den forbindelse ønsker Databeskyttelsesrådet at fremhæve disse underretningers relevans for vurderingen af Republikken Koreas tilstrækkelighed og bemærker f.eks., at underretningerne indeholder relevante præciseringer vedrørende en række vigtige garantier, blandt andet i forbindelse med anvendelsesområdet for undtagelserne fra PIPA i forbindelse med behandling af pseudonymiserede personoplysninger til videnskabelige, forskningsmæssige og statistiske formål, videreoverførsel og de regler, der gælder i forbindelse med offentlige myndigheders indsigt i personoplysninger.

1.2. Udfordringer

9. Selv om Databeskyttelsesrådet har identificeret mange aspekter af Koreas ramme for databeskyttelse som i det væsentlige svarende til den europæiske ramme for databeskyttelse, har det også konkluderet, at der er visse aspekter, der kan kræve en nærmere undersøgelse og præcisering. Konkret finder Databeskyttelsesrådet, at der bør foretages en nærmere vurdering af følgende punkter for at sikre, at det i det væsentlige overensstemmende beskyttelsesniveau overholdes, og at punkterne bør overvåges omhyggeligt af Europa-Kommissionen.

1.2.1. Generelt

10. Databeskyttelsesrådet noterer sig, at underretning nr. 2021-1 *har status som en administrativ regel med juridisk bindende virkning for den persondataansvarlige, i den forstand at enhver overtrædelse af underretningen kan betragtes som en overtrædelse af de relevante bestemmelser i PIPA*[7]. Men da underretningen ikke i sig selv omfatter yderligere regler, men derimod præciseringer af, hvordan PIPA's lovtekst skal anvendes, og i lyset af dens overordnede betydning, navnlig med hensyn til pseudonymiseringsbestemmelserne i henhold til PIPA, som Databeskyttelsesrådet kan forstå er genstand for verserende retssager, opfordrer Databeskyttelsesrådet Europa-Kommissionen til at fremlægge yderligere information om den bindende karakter, muligheden for håndhævelse og gyldigheden af underretning nr. 2021-1 og anbefaler omhyggelig overvågning af den i praksis, navnlig

[7] Jf. afsnit I i bilag I til udkastet til afgørelse.

med hensyn til dens anvendelse ikke alene af den koreanske tilsynsmyndighed, men også af domstole, især hvis det overensstemmende beskyttelsesniveau i Koreas retlige ramme er baseret på de præciseringer, der er indeholdt deri.

1.2.2. Generelle databeskyttelsesmæssige aspekter

11. Med hensyn til anvendelsesområdet for afgørelsen om et tilstrækkeligt beskyttelsesniveau bemærker Databeskyttelsesrådet, at det vil omfatte overførsler fra den retlige ramme for EØS til både offentlige og private "persondataansvarlige", der er omfattet af PIPA. Databeskyttelsesrådet kan forstå, at enheder, der fungerer som databehandlere i den i GDPR anvendte betydning, er omfattet af dette udtryk, men for at undgå misforståelser opfordrer det Europa-Kommissionen til at gøre det klarere, at afgørelsen om et tilstrækkeligt beskyttelsesniveau også vil omfatte overførsler til "databehandlere" i Korea.

12. Et vigtigt aspekt, som Databeskyttelsesrådet ønsker at henlede opmærksomheden på, vedrører begrebet pseudonymiserede personoplysninger i Koreas ramme for databeskyttelse. I henhold til koreansk ret finder undtagelser fra en række relevante bestemmelser, herunder bestemmelser om individuelle registreredes rettigheder samt dataopbevaring, anvendelse på behandlingen af pseudonymiserede personoplysninger. Ifølge Europa-Kommissionen er dette kun tilfældet, når pseudonymiserede personoplysninger behandles til statistiske formål, videnskabelige forskningsformål eller arkivformål i samfundets interesse. Denne påstand understøttes dog hovedsagelig af underretning nr. 2021-1, som gør det allerede nævnte behov for yderligere information om og overvågning af denne underretnings bindende karakter, mulighed for håndhævelse og gyldighed yderst relevant i denne sammenhæng. Desuden opfordrer Databeskyttelsesrådet Europa-Kommissionen til at foretage en nærmere vurdering af konsekvenserne af pseudonymisering i henhold til koreansk ret og, som det vigtigste, hvordan det kan påvirke de grundlæggende rettigheder og frihedsrettigheder for de registrerede, hvis personoplysninger overføres til Republikken Korea i henhold til afgørelsen om et tilstrækkeligt beskyttelsesniveau. Navnlig opfordrer Databeskyttelsesrådet Europa-Kommissionen til at foretage en nærmere vurdering af undtagelserne i artikel 28, stk. 7, i PIPA og artikel 40, stk. 3, i CIA og til at overvåge deres anvendelse samt den relevante retspraksis omhyggeligt med henblik på at sikre, at registreredes rettigheder ikke begrænses i urimelig grad, når personoplysninger, der overføres i henhold til afgørelsen om et tilstrækkeligt beskyttelsesniveau, behandles til disse formål.

13. Databeskyttelsesrådet bemærker endvidere, at der i henhold til koreansk ret kun eksisterer en ret til at trække samtykke tilbage under særlige omstændigheder, og opfordrer derfor Europa-Kommissionen til at foretage en nærmere vurdering af konsekvenserne af manglen på en generel ret til at trække samtykke tilbage samt til at give yderligere sikkerhed for, at det fornødne databeskyttelsesniveau til enhver tid garanteres, også, hvor det er nødvendigt, ved at præcisere den rolle, som retten til suspension i henhold til PIPA spiller, i mangel af en generel ret til at trække samtykke tilbage.

14. Med hensyn til videreoverførsel anerkender Databeskyttelsesrådet, at den registreredes informerede samtykke generelt vil blive anvendt som grundlag for dataoverførsler fra en persondataansvarlig, der er etableret i Republikken Korea, til en modtager, der er etableret i et tredjeland, og at underretning nr. 2021-1 foreskriver, at fysiske personer skal underrettes om det tredjeland, som deres oplysninger vil blive videregivet til. Databeskyttelsesrådet opfordrer imidlertid Europa-Kommissionen til at sikre, at den information, der skal gives til den registrerede, også omfatter information om de mulige risici ved overførsel som følge af manglende tilstrækkelig beskyttelse i tredjelandet samt manglen på fornødne garantier. Databeskyttelsesrådet ser desuden gerne, at der i afgørelsen om et tilstrækkeligt beskyttelsesniveau gives fornyet sikkerhed for, at personoplysninger ikke vil blive overført fra koreanske persondataansvarlige til et tredjeland, i en situation hvor et gyldigt samtykke i henhold til GDPR ikke kan gives, f.eks. på grund af en ulige magtbalance.

15. Med hensyn til udnævnelsen af medlemmerne af den koreanske tilsynsmyndighed ser Databeskyttelsesrådet gerne, selv om den formelle procedure vil være i overensstemmelse med GDPR og derfor opfylde testen af overensstemmelse med den retlige ramme for EØS, at Europa-Kommissionen overvåger enhver udvikling, der kan påvirke uafhængigheden hos medlemmerne af den koreanske tilsynsmyndighed.

16. Med hensyn til budgettet er der, igen på grundlag af information fra Europa-Kommissionen, ingen henvisning til de særlige forhold, der gør sig gældende for de ansatte, der er tilknyttet PIPC, eller til de finansielle ressourcer, der stilles til rådighed for PIPC. Databeskyttelsesrådet ser derfor gerne yderligere information om disse to relevante emner i udkastet til afgørelse.

1.2.3. Om offentlige myndigheders indsigt i personoplysninger, der overføres til Republikken Korea

17. Databeskyttelsesrådet har også analyseret Koreas retlige ramme med hensyn til offentlige myndigheders indsigt i personoplysninger, der overføres fra EØS til Korea, af hensyn til retshåndhævelse og den nationale sikkerhed. Databeskyttelsesrådet anerkender den koreanske regerings bemærkninger og forsikringer, jf. bilag II til udkastet til afgørelse, men har identificeret en række aspekter, der kræver præcisering eller giver anledning til bekymring.

18. Databeskyttelsesrådet bemærker, at PIPA's bestemmelser finder ubegrænset anvendelse på retshåndhævelsesområdet. Databeskyttelsesrådet bemærker også, at databehandling på området national sikkerhed er underlagt en mere begrænset række bestemmelser i PIPA.

19. Med hensyn til teletjenesteudbyderes frivillige videregivelse af personoplysninger til nationale sikkerhedsmyndigheder er Databeskyttelsesrådet bekymret over, at forholdet mellem afsnit 3 i bilag I til udkastet til afgørelse, hvori det præciseres, at udbydere i princippet skal underrette den berørte fysiske person, når de frivilligt efterkommer en anmodning, og artikel 58, stk. 1, litra 2), i PIPA, dvs. den delvise undtagelse af hensyn til den nationale sikkerhed, er uklart. Det kan gøre underretningskravene ineffektive og gøre det betydeligt vanskeligere for registrerede at gøre deres databeskyttelsesrettigheder gældende, navnlig med hensyn til retslig prøvelse.

20. Selv om det ikke udtrykkeligt fremgår af udkastet til afgørelse, kan Databeskyttelsesrådet ud fra Europa-Kommissionens redegørelse forstå, at Koreas retlige ramme ikke giver mulighed for masseaflytning af telekommunikation. Den seneste retspraksis fra Den Europæiske Menneskerettighedsdomstol ("**ECHR**") om masseaflytningssystemer vil derfor ikke være direkte relevant for vurderingen af databeskyttelsesniveauet i Korea.

21. Udkastet til afgørelse indeholder ingen information om de retlige rammer for videreoverførsel på området national sikkerhed. Selv om Databeskyttelsesrådet kunne forstå, at videreoverførsel af hensyn til den nationale sikkerhed efter Europa-Kommissionens opfattelse er tilstrækkeligt reguleret af de generelle garantier og principper, der følger af den forfatningsmæssige ramme og PIPA, er Databeskyttelsesrådet bekymret for, hvorvidt dette kan anses for at opfylde kravene om præcision og klarhed i lovgivningen og sikrer effektive garantier, der kan håndhæves. De garantier, som Kommissionen henviser til, er af meget generel karakter og behandler ikke, i et retsgrundlag, de særlige omstændigheder og betingelser, hvorunder videreoverførsel af hensyn til den nationale sikkerhed kan finde sted. I den forbindelse bemærker Databeskyttelsesrådet også, at Europa-Kommissionen ikke har taget hensyn til eksistensen af internationale aftaler mellem Republikken Korea og tredjelande eller internationale organisationer, der kan fastsætte specifikke bestemmelser for retshåndhævende myndigheders og/eller efterretningstjenesters internationale videregivelse af personoplysninger til tredjelande. Databeskyttelsesrådet finder, at indgåelsen af bilaterale eller multilaterale aftaler med tredjelande med henblik på samarbejde på retshåndhævelses- eller efterretningsområdet må forventes at påvirke Koreas ramme for databeskyttelse som vurderet.

22. Databeskyttelsesrådet bemærker, at tilsynet med de retshåndhævende myndigheder på det strafferetlige område og de nationale sikkerhedsmyndigheder sikres ved en kombination af en række interne og eksterne organer, navnlig PIPC, som har de fornødne udøvende beføjelser.

23. Effektive retsmidler og adgang til retslig prøvelse kræver, at registrerede kan henvende sig til et kompetent organ, der opfylder kravene i artikel 47 i Den Europæiske Unions charter om grundlæggende rettigheder ("**chartret**"), dvs. som har kompetence til at fastslå, at en databehandling finder sted, for at kontrollere behandlingens lovlighed, og som har retsgyldige beføjelser til at træffe afhjælpende foranstaltninger, hvis databehandlingen er ulovlig. På den baggrund anmoder Databeskyttelsesrådet Europa-Kommissionen om at præcisere, om en klage til PIPC eller et søgsmål ved en domstol er underlagt materielle og/eller proceduremæssige krav, såsom en bevisbyrde, og om borgere i EØS vil være i stand til at opfylde en sådan betingelse.

1.3. Konklusion

24. Databeskyttelsesrådet finder, at denne afgørelse om et tilstrækkeligt beskyttelsesniveau er af afgørende betydning, også i betragtning af, at den — med de undtagelser, der er fremhævet i udtalelsen — vil omfatte overførsler både i den offentlige og den private sektor.

25. Databeskyttelsesrådet bifalder den indsats, som Europa-Kommissionen og de koreanske myndigheder har gjort for at tilpasse Koreas retlige ramme til den europæiske. De forbedringer, der agtes indført med underretning nr. 2021-1 for at slå bro over nogle af forskellene mellem de to rammer, er meget vigtige og er blevet godt modtaget. Databeskyttelsesrådet bemærker dog, at der fortsat er en række bekymringer, herunder med hensyn til underretning nr. 2021-1, sammen med behovet for yderligere præcisering af andre spørgsmål, og det anbefaler Europa-Kommissionen at tage hånd om de bekymringer og anmodninger om præcisering, som Databeskyttelsesrådet har fremført, og fremlægge yderligere information og redegørelser vedrørende de spørgsmål, der rejses i denne udtalelse.

2. INDLEDNING

2.1. Koreas ramme for databeskyttelse

26. Den vigtigste lovgivning om databeskyttelse i Republikken Korea er lov om beskyttelse af personoplysninger (lov nr. 10465 af 29. marts 2011, senest ændret ved lov nr. 16930 af 4. februar 2020, "**PIPA**"). Den suppleres af et gennemførelsesdekret (præsidentielt dekret nr. 23169 af 29. september 2011, senest ændret ved præsidentielt dekret nr. 30892 af 4. august 2020, "PIPA-gennemførelsesdekret"), som er juridisk bindende og kan håndhæves.

27. Ud over PIPA omfatter Koreas ramme for databeskyttelse regelfastsættende "underretninger", der udstedes af den koreanske tilsynsmyndighed, kommissionen for beskyttelse af personoplysninger ("**PIPC**") og indeholder yderligere regler for fortolkning og anvendelse af PIPA. PIPC har for nylig vedtaget underretning nr. 2021-1 af 21. januar 2021 (som ændrede den tidligere underretning nr. 2020-10 af 1. september 2020, i det følgende benævnt "**underretning nr. 2021-1**") om fortolkning, anvendelse og håndhævelse af visse bestemmelser i PIPA. Nærmere bestemt var denne underretning resultatet af drøftelser om et tilstrækkeligt beskyttelsesniveau mellem de koreanske myndigheder og Europa-Kommissionen. Den indeholder præciseringer af anvendelsen af specifikke bestemmelser i PIPA, herunder vedrørende behandling af personoplysninger, der overføres til Korea på grundlag af den påtænkte afgørelse om et tilstrækkeligt beskyttelsesniveau[8], og den *har status som en administrativ regel med juridisk bindende virkning for den persondataansvarlige, i den forstand at*

[8] Jf. afsnit I i bilag I til udkastet til afgørelse.

enhver overtrædelse af underretningen kan betragtes som en overtrædelse af de relevante bestemmelser i PIPA[9]. I den forbindelse ønsker Databeskyttelsesrådet at bemærke, at underretningen, selv om den omtales som "supplerende regler" i udkastet til afgørelse, ikke indeholder yderligere regler i sig selv, men derimod redegørelser, der har til formål at præcisere, hvordan PIPA's lovtekst skal anvendes, navnlig når det gælder personoplysninger, der overføres fra EØS. På den baggrund anbefaler Databeskyttelsesrådet omhyggelig overvågning af overholdelsen af underretning nr. 2021-1 i praksis, navnlig med hensyn til dens anvendelse, ikke kun af PIPC, men også af domstole, især når det overensstemmende beskyttelsesniveau i henhold til Koreas retlige ramme er baseret på præciseringerne i underretning nr. 2021-1.

28. Andre relevante databeskyttelseslove i Koreas retlige ramme fastsætter regler for behandling af personoplysninger i specifikke erhvervssektorer såsom:

- lov om anvendelse og beskyttelse af kreditoplysninger ("**CIA**"), herunder dens gennemførelsesdekret ("**CIA-gennemførelsesdekret**"), som fastsætter specifikke regler for kommercielle aktører og specialiserede enheder (såsom kreditvurderingsbureauer og finansielle institutioner), når de behandler kreditrelaterede personoplysninger, der er nødvendige for at fastslå kreditværdigheden hos parter i finansielle eller kommercielle transaktioner
- lov om fremme af anvendelsen af informations- og kommunikationsnetværk og databeskyttelse ("**netværkslov**")
- lov om beskyttelse af personoplysninger i forbindelse med kommunikation ("**CPPA**").

29. På området for offentlige myndigheders indsigt har Databeskyttelsesrådet, ud over de relevante bestemmelser i PIPA og CPPA, taget andre retsakter i betragtning, nærmere bestemt strafferetsplejeloven ("**CPA**"), loven om telekommunikationsvirksomhed ("**TBA**"), loven om indberetning og anvendelse af specifikke oplysninger om finansielle transaktioner ("**ARUSFTI**") og loven om den nationale efterretningstjeneste ("**NISA**").

2.2. Omfanget af Databeskyttelsesrådets vurdering

30. Europa-Kommissionens udkast til afgørelse er resultatet af en vurdering af Koreas ramme for databeskyttelse efterfulgt af drøftelser med den koreanske regering. I henhold til artikel 70, stk. 1, litra s), i GDPR forventes Databeskyttelsesrådet at afgive en uafhængig udtalelse om Europa-Kommissionens resultater, identificere eventuelle mangler i rammen for et tilstrækkeligt beskyttelsesniveau og bestræbe sig på at fremsætte forslag til at afhjælpe disse.

31. For at undgå gentagelser og med det formål at bidrage til vurderingen af Koreas retlige ramme har Databeskyttelsesrådet valgt at fokusere på en række specifikke punkter i udkastet til afgørelse og fremlægge sin analyse og udtalelse om dem og afstå fra at gengive hovedparten af de faktuelle resultater og vurderinger, hvor Databeskyttelsesrådet ikke har grund til at antage, at Republikken Koreas lovgivning i det væsentlige ikke stemmer overens med lovgivningen i EØS. I overensstemmelse med Domstolens retspraksis omfatter en meget vigtig del af analysen desuden de retlige bestemmelser om indsigt i de personoplysninger, der overføres til Republikken Korea af hensyn til den nationale sikkerhed, samt praksis hos landets nationale sikkerhedsapparat.

32. I sin vurdering tog Databeskyttelsesrådet hensyn til den gældende europæiske ramme for databeskyttelse, herunder artikel 7, 8 og 47 i chartret, der beskytter henholdsvis retten til privatliv og familieliv, retten til beskyttelse af personoplysninger og adgangen til effektive retsmidler og til en

[9] Ibid.

upartisk domstol, og artikel 8 i EMRK, der beskytter retten til privatliv og familieliv. Ud over ovenstående gennemgik Databeskyttelsesrådet kravene i GDPR samt den relevante retspraksis.

33. Formålet med denne øvelse er at afgive en udtalelse til Europa-Kommissionen om vurderingen af et tilstrækkeligt beskyttelsesniveau i Republikken Korea. Domstolen har videreudviklet begrebet "tilstrækkeligt beskyttelsesniveau", som allerede fandtes i direktiv 95/46. Det er vigtigt at minde om den standard, der er fastsat af Domstolen i Schrems I, nemlig at "*de retsmidler, som tredjelandet har mulighed for, i denne forbindelse, med henblik på et sådant beskyttelsesniveau, kan afvige fra de retsmidler, der anvendes i EU*", selvom "beskyttelsesniveauet" i tredjelandet "i det væsentlige skal stemme overens" med det niveau, der er garanteret i EU[10]. Målet er derfor ikke at afspejle den europæiske lovgivning punkt for punkt, men at fastlægge de væsentlige og grundlæggende krav i den lovgivning, der undersøges. Et tilstrækkeligt beskyttelsesniveau kan opnås gennem en kombination af rettigheder for de registrerede og forpligtelser for dem, der behandler personoplysninger eller udøver kontrol over en sådan behandling og tilsyn gennem uafhængige organer. Reglerne om databeskyttelse er imidlertid kun effektive, hvis de kan håndhæves, og hvis de følges i praksis. Det er derfor nødvendigt ikke alene at tage indholdet af de regler, der finder anvendelse på personoplysninger, der overføres til et tredjeland eller en international organisation i betragtning, men også det system, der er indført for at sikre reglernes effektivitet. Effektive håndhævelsesmekanismer er af afgørende betydning for databeskyttelsesreglers effektivitet[11].

2.3. Generelle bemærkninger og bekymringer

2.3.1. Internationale forpligtelser indgået af Republikken Korea

34. I henhold til artikel 45, stk. 2, litra c), i GDPR og referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR[12], skal Europa-Kommissionen i sin vurdering af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, blandt andet tage hensyn til de internationale forpligtelser, som tredjelandet har indgået, eller andre forpligtelser, der følger af tredjelandets deltagelse i multilaterale eller regionale systemer, navnlig i forbindelse med beskyttelse af personoplysninger, samt gennemførelsen af sådanne forpligtelser.

35. Korea er part i en række internationale aftaler, der garanterer retten til privatlivets fred, såsom den internationale konvention om borgerlige og politiske rettigheder (artikel 17), konventionen om rettigheder for personer med handicap (artikel 22) og konventionen om barnets rettigheder (artikel 16). Desuden tilslutter Korea sig som OECD-medlem OECD's ramme for databeskyttelse, navnlig retningslinjerne for beskyttelse af personoplysninger og grænseoverskridende udveksling af personoplysninger.

36. Databeskyttelsesrådet noterer sig også Koreas deltagelse som observatørstat i arbejdet i det rådgivende udvalg under Europarådets konvention 108(+), selv om landet endnu ikke har truffet beslutning om tiltrædelse.

2.3.2. Anvendelsesområdet for afgørelsen om et tilstrækkeligt beskyttelsesniveau

37. I henhold til betragtning 5 i udkastet til afgørelse konkluderer Europa-Kommissionen, at Republikken Korea sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra en dataansvarlig eller databehandler i Unionen til persondataansvarlige (f.eks. fysiske eller juridiske

[10] C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6. oktober 2015, ECLI:EU:C:2015:650, præmis 73-74.
[11] WP254, s. 2.
[12] WP254, s. 2.

personer, organisationer, offentlige institutioner), der er omfattet af PIPA's anvendelsesområde, med undtagelse af behandling af personoplysninger i forbindelse med religiøse organisationers missionsaktiviteter og politiske partiers opstilling af kandidater[13], eller behandling af kreditrelaterede personoplysninger i henhold til CIA foretaget af dataansvarlige, der er underlagt det sydkoreanske finanstilsyns tilsyn.

38. Databeskyttelsesrådet bemærker, at afgørelsen om et tilstrækkeligt beskyttelsesniveau vil omfatte overførsler fra den retlige ramme for EØS til både offentlige og private "persondataansvarlige", der er omfattet af PIPA. Databeskyttelsesrådet kan forstå, at enheder, der fungerer som databehandlere i den i GDPR anvendte betydning, også er omfattet af udtrykket "persondataansvarlig", da PIPA vil finde tilsvarende anvendelse på dem, og at der gælder specifikke forpligtelser, når en persondataansvarlig ("outsourcer") lader en tredjemand behandle personoplysninger ("underleverandør"), men for at undgå misforståelser opfordrer Databeskyttelsesrådet Europa-Kommissionen til at gøre det klarere, at afgørelsen om et tilstrækkeligt beskyttelsesniveau også vil omfatte overførsler til "databehandlere" i Korea, og at niveauet for beskyttelse af personoplysninger, der overføres fra EØS, heller ikke undermineres i disse tilfælde.

39. I betragtning af, at afgørelsen om et tilstrækkeligt beskyttelsesniveau også omfatter overførsel af personoplysninger mellem offentlige organer, kan Databeskyttelsesrådet desuden forstå, at dette også vil omfatte overførsler mellem tilsynsmyndigheder på databeskyttelsesområdet, og opfordrer af klarhedshensyn Europa-Kommissionen til specifikt at behandle dette spørgsmål.

40. For så vidt angår de enheder, der ikke er omfattet af anvendelsesområdet for afgørelsen om et tilstrækkeligt beskyttelsesniveau, vil Databeskyttelsesrådet desuden gerne understrege, at afgørelsen om et tilstrækkeligt beskyttelsesniveau kan drage fordel af en klarere identifikation af de "kommercielle organisationer", der er underlagt PIPC's tilsyn (artikel 45, stk. 3, i CIA), således at dataansvarlige og databehandlere, der er etableret i EØS, let kan vurdere, om importøren også er omfattet af anvendelsesområdet for afgørelsen om et tilstrækkeligt beskyttelsesniveau, inden de overfører personoplysninger til enheder, der er omfattet af CIA's anvendelsesområde, eller i det mindste gøres opmærksom på behovet for at vurdere dette aspekt.

41. Med hensyn til anvendelsesområdet for afgørelsen om et tilstrækkeligt beskyttelsesniveau kunne Databeskyttelsesrådet ud fra Europa-Kommissionens supplerende redegørelse forstå, at Koreas finansielle efterretningsenhed ("**KOFIU**"), der er oprettet under det sydkoreanske finanstilsyn og fører tilsyn med forebyggelsen af hvidvask og finansiering af terrorisme i henhold til ARUSFTI[14], heller ikke er omfattet af anvendelsesområdet, da den kun har jurisdiktion over finansielle institutioner, som ikke selv er omfattet af udkastet til afgørelse. Imidlertid er det i henhold til artikel 1, stk. 2, litra c), i udkastet til afgørelse kun de persondataansvarlige, der er underlagt det sydkoreanske finanstilsyns tilsyn og behandler kreditrelaterede personoplysninger i henhold til CIA, som ikke er omfattet af dens anvendelsesområde. På den baggrund anmoder Databeskyttelsesrådet Europa-Kommissionen om at præcisere, om KOFIU og de databehandlingsaktiviteter, der udføres af KOFIU selv, er omfattet af udkastet til afgørelse.

3. GENERELLE DATABESKYTTELSESMÆSSIGE ASPEKTER

3.1. Indholdsmæssige principper

42. Kapitel 3 i referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR omhandler "indholdsmæssige principper". Et tredjelands system skal indeholde disse principper for at anse det

[13] Yderligere kontekst kan findes nedenfor i afsnit 3.1.2 i denne udtalelse.
[14] Jf. bilag II, afsnit 2.2.3.1.

fastsatte beskyttelsesniveau for i det væsentlige at stemme overens med det niveau, der garanteres i EU-retten.

43. Selv om retten til beskyttelse af personoplysninger ikke udtrykkeligt er forankret i Koreas forfatning i sig selv, anerkendes den som en grundlæggende rettighed, der er afledt af de forfatningsmæssige rettigheder til menneskelig værdighed og forfølgelse af lykke (artikel 10), privatliv (artikel 17) og privatlivets fred i forbindelse med kommunikation (artikel 18). Dette er blevet bekræftet af både den øverste domstol og forfatningsdomstolen, som anført i Europa-Kommissionens udkast til afgørelse[15]. Databeskyttelsesrådet noterer sig denne anerkendelse, da det udleder heraf, at databeskyttelse som en grundlæggende rettighed i henhold til artikel 37 i Koreas forfatning "*kun kan begrænses ved lov, og når det er nødvendigt af hensyn til den nationale sikkerhed, opretholdelse af lov og orden eller den offentlige velfærd*", og at "*selv om sådanne begrænsninger pålægges, må de ikke berøre kernen i rettighederne og frihedsrettighederne*".

44. Ifølge Europa-Kommissionen[16] har forfatningsdomstolen fastslået, at også udenlandske statsborgere har grundlæggende rettigheder. Selv om retspraksis hidtil ikke specifikt har behandlet ikke-koreanske statsborgeres ret til privatlivets fred, er det ifølge de officielle erklæringer fra den koreanske regering[17] almindeligt anerkendt blandt forskere, at artikel 12-22 i forfatningen omhandler "menneskers rettigheder". Endvidere har Republikken Korea vedtaget en række love på databeskyttelsesområdet, som indeholder garantier for alle fysiske personer, uanset deres nationalitet, såsom PIPA. I den forbindelse noterer Databeskyttelsesrådet sig, at artikel 6, stk. 2, i forfatningen fastsætter, at udenlandske statsborgeres status er garanteret i overensstemmelse med folkeretten og internationale traktater samt i den retspraksis, der er nævnt i udkastet til afgørelse, i henhold til hvilken en "udlænding" kan være indehaver af "grundlæggende rettigheder". I betragtning af relevansen af anerkendelsen af retten til beskyttelse af personoplysninger for "udenlandske statsborgere" henleder Databeskyttelsesrådet Europa-Kommissionens opmærksomhed på behovet for fortsat at overvåge retspraksis vedrørende beskyttelse af personoplysninger som en grundlæggende rettighed, der ikke kun anerkendes for koreanske borgere, men for alle registrerede, med henblik på at sikre, at det beskyttelsesniveau for fysiske personer, der garanteres i GDPR, ikke undermineres, når personoplysninger overføres til Korea i henhold til afgørelsen om et tilstrækkeligt beskyttelsesniveau.

3.1.1. Begreber

45. På grundlag af referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR bør tredjelandets retlige rammer indeholde grundlæggende databeskyttelsesbegreber og/eller -principper. Selv om disse ikke skal afspejle terminologien i GDPR, bør de afspejle og være i overensstemmelse med de begreber, der er forankret i den europæiske databeskyttelseslovgivning. F.eks. indeholder GDPR følgende vigtige begreber: "personoplysninger", "behandling af personoplysninger", "dataansvarlig", "databehandler", "modtager" og "følsomme oplysninger"[18].

46. PIPA omfatter en række definitioner såsom "personoplysninger", "behandling" og "den registrerede", som ligger tæt op ad de tilsvarende udtryk i GDPR.

3.1.1.1. Begrebet pseudonymiserede personoplysninger

47. Blandt definitionerne i PIPA definerer artikel 2, stk. 1, i PIPA navnlig personoplysninger som enhver af følgende oplysninger om en levende person: a) oplysninger, der identificerer en bestemt person ved

[15] Jf. betragtning 8 i udkastet til afgørelse og den relevante retspraksis, som der henvises til i fodnote 10 i udkastet til afgørelse, og hvoraf der kun findes resuméer på engelsk.
[16] Jf. betragtning 9 i udkastet til afgørelse.
[17] Afsnit 1.1. i bilag II til udkastet til afgørelse.
[18] WP254, s. 4.

hjælp af den pågældendes fulde navn, personregistreringsnummer, billede osv., og b) oplysninger, som, selv om de ikke i sig selv identificerer en bestemt person, let kan kombineres med andre oplysninger med henblik på at identificere en bestemt person. I sidstnævnte tilfælde afgøres det, om det er let at kombinere oplysninger, under rimelig hensyntagen til den tid, omkostning, teknologi osv., der er anvendt til at identificere den pågældende, såsom sandsynligheden for, at de øvrige oplysninger kan fremskaffes.

48. Desuden fremgår det af artikel 2, stk. 1, litra c), i PIPA, at også "pseudonymiserede personoplysninger" anses for at være personoplysninger. Pseudonymiserede oplysninger defineres som oplysninger under punkt a) eller b) ovenfor, som pseudonymiseres i overensstemmelse med underafsnit 1-2 og derved ikke kan anvendes til at identificere en bestemt person uden brug eller kombination af oplysninger til at genoprette den oprindelige tilstand. Oplysninger, der er fuldt anonymiserede, er ikke omfattet af PIPA's anvendelsesområde. I henhold til artikel 58, stk. 2, i PIPA finder loven ikke anvendelse på oplysninger, der ikke længere identificerer en bestemt person, når de kombineres med andre oplysninger, under rimelig hensyntagen til tid, omkostninger, teknologi osv.

49. Europa-Kommissionen anfører i betragtning 17 i sit udkast til afgørelse, at dette svarer til det materielle anvendelsesområde for GDPR og dens begreber "personoplysninger", "pseudonymisering" og "anonymiserede oplysninger".

50. I henhold til artikel 28, stk. 7, i PIPA finder artikel 20, 21, 27, artikel 34, stk. 1, artikel 35-37, artikel 39, stk. 3, artikel 39, stk. 4, og artikel 39, stk. 6-8, ikke anvendelse på pseudonymiserede personoplysninger.

51. Europa-Kommissionen anfører i sit udkast til afgørelse, at artikel 28, stk. 7, i PIPA kun finder anvendelse på pseudonymiserede personoplysninger, når de behandles til statistiske formål, videnskabelige forskningsformål eller arkivformål i samfundets interesse[19]. Dette følger imidlertid ikke direkte af lovens bogstav, men af redegørelserne i underretning nr. 2021-1[20]. Databeskyttelsesrådet anerkender, at der kan fremsættes et argument baseret på PIPA's struktur og rationale om, at artikel 28, stk. 2, i PIPA skal forstås og logisk fortolkes på en måde, så den også finder anvendelse på artikel 28, stk. 7, i PIPA, i lyset af betydningen af underretning nr. 2021-1 i Europa-Kommissionens vurdering af, om beskyttelsesniveauet for personoplysninger i Republikken Korea er tilstrækkeligt, og for at undgå enhver tvivl opfordrer Databeskyttelsesrådet Europa-Kommissionen til at fremlægge yderligere information om den bindende karakter, muligheden for håndhævelse og gyldigheden af underretning nr. 2021-1 og til at overvåge dens anvendelse i denne specifikke sammenhæng.

52. I den forbindelse vil Databeskyttelsesrådet gerne minde om, at pseudonymisering i henhold til GDPR forstås som en anbefalet sikkerhedsforanstaltning. Med andre ord forbliver pseudonymiserede personoplysninger i henhold til GDPR personoplysninger, som GDPR finder fuld anvendelse på. På baggrund af ovenstående er Databeskyttelsesrådet bekymret for, at GDPR's beskyttelsesniveau for pseudonymiserede personoplysninger kan undermineres, når personoplysninger overføres til Korea. Derfor opfordrer Databeskyttelsesrådet Europa-Kommissionen til at foretage en nærmere vurdering af konsekvenserne af pseudonymisering i henhold til PIPA og, som det vigtigste, hvordan pseudonymisering kan påvirke de grundlæggende rettigheder og frihedsrettigheder for registrerede, hvis personoplysninger overføres til Republikken Korea på grundlag af afgørelsen om et tilstrækkeligt beskyttelsesniveau. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at give sikkerhed for, at beskyttelsesniveauet for personoplysninger fra registrerede i EØS ikke vil blive

[19] Se blandt andet betragtning 82 i udkastet til afgørelse.
[20] Afsnit 4 i bilag I til udkastet til afgørelse.

sænket efter overførslen til Republikken Korea, selv når de overførte personoplysninger pseudonymiseres.

3.1.1.2. *Begrebet persondataansvarlig*

53. Artikel 2, stk. 5, i PIPA indeholder følgende definition af "persondataansvarlig": en offentlig institution, juridisk person, organisation eller fysisk person osv., der behandler personoplysninger direkte eller indirekte med henblik på at administrere persondatafiler "*som led i sine aktiviteter*". I de supplerende garantier, der er fastsat i underretning nr. 2021-1, defineres udtrykket "persondataansvarlig" imidlertid som en offentlig institution, juridisk person, organisation, fysisk person osv., der behandler personoplysninger direkte eller indirekte med henblik på at administrere persondatafilerne "*til forretningsmæssige formål*". I stedet anføres følgende i fodnote 272 i udkastet til afgørelse om begrebet persondataansvarlig: "*Som defineret i artikel 2 i PIPA, dvs. en offentlig institution, juridisk person, organisation, fysisk person osv., der behandler personoplysninger direkte eller indirekte med henblik på at administrere persondatafiler 'til officielle eller forretningsmæssige formål'.*"

54. Databeskyttelsesrådet anerkender, at disse uoverensstemmelser kan skyldes oversættelser af originalteksten som stillet til rådighed af de koreanske myndigheder, og opfordrer Europa-Kommissionen til løbende at kontrollere oversættelsernes kvalitet og pålidelighed. Databeskyttelsesrådet understreger dog, at det er nødvendigt at have en klar forståelse af de behandlingsformål, der er omfattet af PIPA's materielle anvendelsesområde, for at kunne vurdere, om beskyttelsesniveauet i Koreas retlige ramme i det væsentlige stemmer overens med niveauet i EU-retten. I den forbindelse bemærker Databeskyttelsesrådet endvidere, at der i PIPA ikke anvendes samme terminologi som i GDPR, hvad angår begreberne "dataansvarlig" og "databehandler", og opfordrer Europa-Kommissionen til at præcisere den korrekte definition og anvendelsesområdet af begrebet "dataansvarlig" og specifikt tage stilling til, om dette udtryk også omfatter databehandlere i den i GDPR anvendte betydning, da dette direkte påvirker anvendelsesområdet for afgørelsen om et tilstrækkeligt beskyttelsesniveau[21].

3.1.2. Delvise undtagelser i henhold til PIPA

55. Dele af PIPA (dvs. artikel 15-57) finder ifølge artikel 58, stk. 1, i PIPA ikke anvendelse på fire kategorier af behandling af personoplysninger som beskrevet nedenfor. Nærmere bestemt vedrører undtagelserne bestemmelserne i PIPA om specifikke grunde til behandling, bestemte databeskyttelsesforpligtelser, de nærmere regler for udøvelse af individuelle rettigheder samt reglerne for tvistbilæggelse. Databeskyttelsesrådet noterer sig imidlertid, at visse generelle bestemmelser i PIPA stadig finder anvendelse, herunder bestemmelser, der vedrører databeskyttelsesprincipperne (artikel 3 i PIPA) og individuelle rettigheder (artikel 4 i PIPA). Desuden fastsætter artikel 58, stk. 4, i PIPA specifikke forpligtelser for disse fire kategorier af databehandling.

56. For det første omfatter den delvise undtagelse personoplysninger, der indsamles i henhold til statistikloven med henblik på behandling i offentlige institutioner. Europa-Kommissionen anfører i betragtning 27 i sit udkast til afgørelse, at personoplysninger, der behandles i denne forbindelse, ifølge præciseringer modtaget fra den koreanske regering normalt vedrører koreanske statsborgere og kun undtagelsesvis kan omfatte oplysninger om udlændinge, nemlig i tilfælde af statistikker over indrejse til og udrejse fra territoriet eller om udenlandske investeringer. Ifølge udkastet til afgørelse overføres sådanne oplysninger, selv i disse situationer, normalt ikke fra dataansvarlige/databehandlere i EØS, men vil derimod blive indsamlet direkte af offentlige myndigheder i Korea.

57. Databeskyttelsesrådet anerkender Europa-Kommissionens begrundelse for, at statistikloven ikke finder anvendelse på behandling af personoplysninger, der overføres i henhold til afgørelsen om et tilstrækkeligt beskyttelsesniveau; det ser dog gerne yderligere information om og fornyet sikkerhed

[21] Jf. også punkt 38 ovenfor.

for de specifikke garantier, der vil finde anvendelse, hvis personoplysninger, der overføres fra EØS, desuden indsamles i henhold til statistikloven med henblik på behandling i offentlige institutioner, navnlig vedrørende registreredes udøvelse af individuelle rettigheder i henhold til artikel 89, stk. 2, i GDPR, for så vidt som sådanne rettigheder må forventes ikke at gøre det umuligt eller i alvorlig grad hindre opfyldelsen af de specifikke formål, og sådanne undtagelser ikke er nødvendige for opfyldelsen af disse formål.

58. I dette perspektiv synes anvendelsen af artikel 4 i PIPA også på denne type behandling at give fornyet sikkerhed, men Databeskyttelsesrådet ser gerne yderligere information og præciseringer i afgørelsen om et tilstrækkeligt beskyttelsesniveau vedrørende de specifikke forpligtelser, der i henhold til artikel 58, stk. 4, i PIPA pålægges disse behandlingsaktiviteter, dvs. med hensyn til dataminimering, begrænset dataopbevaring, sikkerhedsforanstaltninger og behandling af klager.

59. For det andet omfatter den delvise undtagelse personoplysninger, der indsamles eller ønskes stillet til rådighed med henblik på analyse af oplysninger vedrørende den nationale sikkerhed. Databeskyttelsesrådet er klar over, at stater i sager, der vedrører den nationale sikkerhed, har en bred skønsmargen, som anerkendes af Menneskerettighedsdomstolen. Databeskyttelsesrådet bemærker også, at enhver begrænsning af rettigheder og frihedsrettigheder, f.eks. når det er nødvendigt for at beskytte den nationale sikkerhed, i henhold til artikel 37, stk. 2, i Koreas forfatning ikke må krænke det væsentlige aspekt, som disse rettigheder og frihedsrettigheder udgør. Endvidere noterer Databeskyttelsesrådet sig garantierne i afsnit 6 i underretning nr. 2021-1 vedrørende behandling af personoplysninger af hensyn til den nationale sikkerhed, herunder efterforskning af overtrædelser samt håndhævelse. I den forbindelse opfordrer Databeskyttelsesrådet dog Europa-Kommissionen til at præcisere undtagelsernes anvendelsesområde nærmere, da det er i tvivl om, hvorvidt alle undtagelserne i artikel 58, stk. 1, litra 2), i PIPA (kapitel III-VII) er relevante for efterretningstjenesters arbejde, og hvorvidt de sikrer overensstemmelse med nødvendigheds- og proportionalitetsprincippet. Databeskyttelsesrådet opfordrer navnlig Europa-Kommissionen til at præcisere nærmere, under hvilke omstændigheder en efterretningstjeneste kan påberåbe sig undtagelserne. Databeskyttelsesrådet finder det nødvendigt at overvåge konsekvenserne af disse begrænsninger omhyggeligt i praksis, navnlig hvad angår effektiv udøvelse og håndhævelse af registreredes rettigheder.

60. For det tredje finder den delvise undtagelse anvendelse på "*personoplysninger, der behandles midlertidigt, når det er bydende nødvendigt af hensyn til den offentlige sikkerhed, folkesundheden osv.*" Ifølge betragtning 29 i Europa-Kommissionens udkast til afgørelse fortolkes denne kategori strengt af PIPC og gælder kun i nødsituationer, der kræver hasteforanstaltninger, f.eks. for at spore infektiøse stoffer eller redde og hjælpe ofre for naturkatastrofer.

61. Databeskyttelsesrådet understreger også, at eventuelle undtagelser fra beskyttelsesniveauet for personoplysninger bør fortolkes strengt. Samtidig bemærker Databeskyttelsesrådet, at bestemmelsen ikke er nøje defineret og ikke indeholder en udtømmende liste over eksempler på situationer, hvor behandling af personoplysninger kan anses for at være "*bydende nødvendig*t". F.eks. er Databeskyttelsesrådet bekymret for, om internationale overførsler af sundhedsdata under den igangværende covid-19-pandemi også vil være omfattet af denne undtagelses anvendelsesområde. I lyset af ovenstående opfordrer Databeskyttelsesrådet Europa-Kommissionen til at præcisere anvendelsesområdet for denne undtagelse nærmere og til fuldt ud at overvåge dens anvendelse og anvendelsesområde for at sikre, at den ikke fører til, at beskyttelsesniveauet for personoplysninger fra EØS sænkes efter overførsel til Korea på grundlag af afgørelsen om et tilstrækkeligt beskyttelsesniveau.

62. Endelig finder den delvise undtagelse anvendelse på personoplysninger, der indsamles eller anvendes med henblik på pressens rapportering, religiøse organisationers missionsaktiviteter og politiske

partiers opstilling af kandidater[22]. Med hensyn til pressens behandling af personoplysninger med henblik på journalistiske aktiviteter anfører Europa-Kommissionen i betragtning 31 i sit udkast til afgørelse, at balancen mellem ytringsfrihed og andre rettigheder, herunder retten til privatlivets fred, er fastsat i loven om voldgift og retsmidler osv. for skader forvoldt af presserapporter (herefter "**presselov**") og nævner specifikke garantier, der følger af presseloven. Databeskyttelsesrådet opfordrer dog Europa-Kommissionen til at overvåge denne undtagelse og den relevante retspraksis fuldt ud med henblik på at sikre, at der også i praksis sikres et databeskyttelsesniveau i Koreas retlige ramme, der stemmer overens med niveauet i EU-retten.

3.1.3. Grundlag for lovlig og rimelig behandling til legitime formål

63. Ifølge referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR skal personoplysninger, i lighed med GDPR, behandles lovligt, rimeligt og legitimt. Retsgrundlaget for lovlig, rimelig og legitim behandling af personoplysninger bør være fastlagt på en tilstrækkeligt klar måde. Den europæiske ramme anerkender en række former for legitime grundlag, herunder f.eks. bestemmelser i national lovgivning, den registreredes samtykke, opfyldelse af en kontrakt eller den dataansvarliges eller en tredjemands legitime interesse, som ikke går forud for den fysiske persons interesser.

64. PIPA indfører, i lighed med strukturen i GDPR, princippet om lovlighed, rimelighed og gennemsigtighed allerede i begyndelsen (artikel 3, stk. 1 og 2, i PIPA) og fastsætter de specifikke regler for dets anvendelse senere (artikel 15-19 i PIPA). Nærmere bestemt indeholder artikel 15 i PIPA et katalog over retsgrundlag, som persondataansvarlige kan basere indsamlingen af personoplysninger på og anvende dem inden for rammerne af formålet med indsamling. Retsgrundlagene omfatter 1) den registreredes informerede samtykke, 2) lovbestemt tilladelse eller nødvendighed for at overholde en retlig forpligtelse, 3) nødvendighed for en offentlig institutions varetagelse af sine opgaver, 4) nødvendighed for at indgå eller opfylde en kontrakt med en registreret, 5) nødvendighed for at beskytte den registreredes eller en tredjemands liv, helbred eller ejendom mod overhængende fare (og forudgående samtykke ikke kan indhentes), 6) nødvendighed for at opfylde en persondataansvarligs berettigede interesse, der har forrang for den registreredes.

65. I artikel 17 i PIPA oplistes retsgrundlagene for videregivelse af personoplysninger til en tredjemand. De omfatter 1) den registreredes informerede samtykke, 2) lovbestemt tilladelse eller nødvendighed for at overholde en retlig forpligtelse, 3) nødvendighed for en offentlig institutions varetagelse af sine opgaver, 4) nødvendighed for at beskytte den registreredes eller en tredjemands liv, helbred eller ejendom mod overhængende fare (og forudgående samtykke ikke kan indhentes). Selv i mangel af den registreredes samtykke er videregivelse af personoplysninger tilladt, hvis dette sker inden for de rammer, der med rimelighed kan henføres til de formål, hvortil personoplysningerne oprindeligt blev indsamlet (artikel 17, stk. 4, i PIPA).

66. Artikel 18 i PIPA fastsætter specifikke regler for anvendelse og videregivelse af personoplysninger, når dette ikke er omfattet af det oprindelige formål med indsamlingen eller afgivelsen. Også her udgør blandt andet samtykke et sådant retsgrundlag.

67. Databeskyttelsesrådet anerkender Koreas lovgivnings betydelige lighed med GDPR med hensyn til princippet om lovlighed og eksistensen af en generel ret til suspension (artikel 37 i PIPA), som også kan påberåbes, når personoplysninger behandles på grundlag af samtykke, men vil gerne bemærke,

[22] Religiøse organisationers behandling af personoplysninger med henblik på missionsaktiviteter samt politiske partiers behandling af personoplysninger i forbindelse med opstilling af kandidater er derfor heller ikke omfattet af anvendelsesområdet for afgørelsen om et tilstrækkeligt beskyttelsesniveau. Jf. også punkt 37 ovenfor i afsnit 2.3.2.

at der i PIPA ikke findes en generel ret til at trække samtykke tilbage[23]. I lyset af betydningen af samtykke som retsgrundlag i alle ovennævnte scenarier og under hensyntagen til den rolle, som individuelle rettigheder spiller i et retssystem med databeskyttelse for at beskytte de registreredes grundlæggende rettigheder og frihedsrettigheder, opfordrer EDPR Europa-Kommissionen til at foretage en nærmere vurdering af konsekvenserne af en manglende generel ret til at trække samtykke tilbage i Koreas lovgivning samt til at give yderligere sikkerhed for, at et grundlæggende databeskyttelsesniveau som det databeskyttelsesniveau, der er fastsat i GDPR, til enhver tid er garanteret, også, hvis det er nødvendigt, ved at præcisere den rolle, retten til suspension spiller i denne specifikke sammenhæng.

3.1.4. Princippet om formålsbegrænsning

68. Referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR fastsætter, på linje med GDPR, at personoplysninger skal behandles til et specifikt formål og efterfølgende udelukkende anvendes, såfremt anvendelsen ikke er uforenelig med formålet med behandlingen.

69. I henhold til artikel 3, stk. 1 og 2, i PIPA skal persondataansvarlige angive og tydeliggøre formålene med behandlingen og sikre, at behandlingen er forenelig med disse formål. Selv om dette princip bekræftes i andre bestemmelser (dvs. artikel 15, stk. 1, artikel 18, stk. 1, og artikel 19, stk. 1, i PIPA), er behandling til "rimeligt relaterede" formål tilladt under visse omstændigheder (jf. artikel 17, stk. 4, i PIPA)[24], hvilket også gælder anvendelse og afgivelse af personoplysninger uden for formålet (jf. artikel 18 og 19 i PIPA)[25].

70. Databeskyttelsesrådet kan forstå, at i tilfælde af overførsel af personoplysninger fra EØS til Republikken Korea på grundlag af afgørelsen om et tilstrækkeligt beskyttelsesniveau udgør formålet med de i EØS etablerede dataansvarliges indsamling det formål, hvortil oplysningerne overføres, og som finder anvendelse på den modtagende i Korea etablerede persondataansvarliges behandling. En ændring af formålet fra den i Korea etablerede dataansvarliges side vil kun være tilladt som fastsat i artikel 18, stk. 2, litra 1)-3), i PIPA, "*medmindre det er sandsynligt, at dette vil krænke en registrerets eller en tredjemands interesser på urimelig vis*"[26]. I den forbindelse anerkender Databeskyttelsesrådet Europa-Kommissionens erklæring i betragtning 55 i udkastet til afgørelse om, at når ændringer af formål er tilladt ved lov, skal de pågældende love respektere den grundlæggende ret til privatlivets fred og beskyttelse af personoplysninger. EDPR bemærker imidlertid, at der ikke er fremlagt specifik information til underbygning af denne bestemte erklæring, f.eks. er der ikke henvist til artikel 37 i Koreas forfatning. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at give yderligere sikkerhed og garantier i udkastet til afgørelse for at sikre, at enhver lovgivning, der tillader en ændring af behandlingens formål, respekterer registreredes grundlæggende rettigheder og frihedsrettigheder med hensyn til privatlivets fred og beskyttelse af personoplysninger.

---

[23] Selv om registrerede under visse omstændigheder kan nægte samtykke, jf. f.eks. artikel 18, stk. 3, litra 5), i PIPA. Derimod synes retten til at trække sit samtykke tilbage kun at eksistere i særlige tilfælde; i henhold til artikel 27, stk. 1, litra 2), i PIPA har registrerede ret til at trække deres samtykke tilbage, hvis de ikke ønsker, at deres personoplysninger videregives til tredjemand som følge af overførsel af en del af eller hele den persondataansvarliges virksomhed, en fusion osv.; i henhold til artikel 39, stk. 7, i PIPA kan brugere til enhver tid trække deres samtykke til indsamling, anvendelse og levering af personoplysninger tilbage fra udbydere af informations- og kommunikationstjenester osv.; og i henhold til artikel 37 i CIA kan en person, der er genstand for kreditvurdering, trække det samtykke tilbage, der er givet til en udbyder/bruger af kreditoplysninger.

[24] Hvor forenelighed med formålet skal fastslås på forhånd på grundlag af kriterierne i artikel 14-2 i PIPA-gennemførelsesdekretet.

[25] Jf. også punkt 66 ovenfor.

[26] Artikel 18, stk. 2, i PIPA.

3.1.5. Princippet om datakvalitet og proportionalitet

71. I referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR er det anført, at personoplysninger skal være korrekte og om nødvendigt ajourførte. De skal være tilstrækkelige, relevante og ikke for omfattende i forhold til de formål, hvortil de behandles.

72. I henhold til PIPA skal persondataansvarlige sikre, at personoplysninger er korrekte, fuldstændige og ajourførte i det omfang, det er nødvendigt i forhold til de formål, hvortil personoplysningerne behandles (artikel 3, stk. 3, i PIPA). Dataansvarlige skal indsamle så få personoplysninger som muligt for at opfylde et bestemt formål. De bærer bevisbyrden i den henseende (artikel 16, stk. 1, i PIPA).

73. På den baggrund deler Databeskyttelsesrådet Europa-Kommissionens vurdering med hensyn til, om beskyttelsesniveauet i henhold til PIPA i det væsentlige stemmer overens med niveauet i GDPR i denne henseende.

3.1.6. Princippet om dataopbevaring

74. Ifølge referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR bør personoplysninger generelt ikke opbevares i et længere tidsrum end det, der er nødvendigt til de formål, hvortil personoplysningerne behandles. Dette princip findes også i koreansk ret, jf. artikel 21, stk. 1, i PIPA. I henhold til PIPA skal persondataansvarlige tilintetgøre personoplysninger straks, når personoplysningerne ikke længere er nødvendige, ved udløbet af opbevaringsperioden, eller når det tilsigtede formål med behandlingen er opfyldt, medmindre de lovbestemte opbevaringsperioder finder anvendelse.

75. EDPR er imidlertid bekymret over, at artikel 21, stk. 1, i PIPA ikke finder anvendelse på pseudonymiserede personoplysninger. EDPR noterer sig, at det af afsnit 4, nr. iii), i underretning nr. 2021-1, fremgår, at "*hvis en persondataansvarlig behandler pseudonymiserede personoplysninger med henblik på at udarbejde statistikker, drive videnskabelig forskning, opbevare offentlige registre osv., og hvis de pseudonymiserede personoplysninger ikke er blevet* [sic] *tilintetgjort, når det specifikke formål med behandlingen er opfyldt, i overensstemmelse med artikel 37 i forfatningen og artikel 3 (principper for beskyttelse af personoplysninger) i loven, skal den persondataansvarlige anonymisere oplysningerne med henblik på at sikre, at de ikke længere identificerer en specifik person, alene eller i kombination med andre oplysninger, under rimelig hensyntagen til tid, omkostninger, teknologi osv., i overensstemmelse med artikel 58, stk. 2, i PIPA.*" I betragtning af, også her, vigtigheden af underretning 2021-1 og med henblik på at beskytte retssikkerheden med hensyn til, om beskyttelsesniveauet for personoplysninger, der overføres til Republikken Korea på grundlag af afgørelsen om tilstrækkelighed, i det væsentlige stemmer overens med niveauet i EU-retten, gentager Databeskyttelsesrådet sin opfordring til Europa-Kommissionen om specifikt at give yderligere information om, hvordan underretning nr. 2021-1 er gjort bindende, og hvordan dens mulighed for håndhævelse og gyldighed sikres[27].

3.1.7. Princippet om sikkerhed og fortrolighed

76. Som beskrevet i referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR kræver princippet om sikkerhed og fortrolighed, at enhver enhed, som behandler personoplysninger, bør sikre, at oplysningerne behandles på en måde, der garanterer personoplysningernes sikkerhed, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger. I forbindelse med sikkerhedsniveauet bør det aktuelle tekniske niveau og de dermed forbundne omkostninger tages i betragtning.

[27] Jf. også punkt 51 ovenfor i afsnit 3.1.1.1 i denne udtalelse samt punkt 52 vedrørende Databeskyttelsesrådets generelle bekymring med hensyn til konsekvenserne af pseudonymisering i henhold til koreansk ret.

77. Europa-Kommissionen har identificeret et lignende princip om datasikkerhed i artikel 3, stk. 4, i PIPA, som er nærmere præciseret i artikel 29 i PIPA. Desuden finder bestemmelserne om datasikkerhed anvendelse, når den persondataansvarlige gør brug af en "underleverandør". Sikkerheden i forbindelse med behandlingen skal sikres gennem tekniske og administrative sikkerhedsforanstaltninger, som også skal indgå i den bindende databehandlingsaftale (artikel 26 i PIPA og artikel 28 i PIPA-gennemførelsesdekretet). Endvidere gælder der i henhold til PIPA særlige forpligtelser i tilfælde af brud på datasikkerheden, herunder forpligtelsen til at underrette berørte registrerede og tilsynsmyndigheden, hvis antallet af berørte registrerede overstiger den gældende tærskel (artikel 34 i PIPA sammenholdt med artikel 39 i det præsidentielle PIPA-dekret), medmindre de berørte oplysninger er pseudonymiserede personoplysninger, der behandles til statistiske formål, videnskabelige forskningsformål eller arkivformål i offentlighedens interesse (artikel 28, stk. 7, i PIPA). Også her er[28] Databeskyttelsesrådet bekymret over de vidtrækkende undtagelser for pseudonymiserede personoplysninger og gentager sin opfordring til Europa-Kommissionen om at foretage en nærmere vurdering af dette aspekt med henblik på at sikre, at der i henhold til koreansk ret er fastsat et beskyttelsesniveau, der i det væsentlige stemmer overens med niveauet i EU-retten[29].

78. Desuagtet er Databeskyttelsesrådet alt i alt tilfreds med Europa-Kommissionens vurdering og konklusion med hensyn til, om Koreas lovgivning i det væsentlige stemmer overens med niveauet i EU-retten, når det gælder princippet om sikkerhed og fortrolighed.

3.1.8. Princippet om gennemsigtighed

79. I henhold til artikel 5, stk. 1, litra a), i GDPR er gennemsigtighed et grundlæggende princip i EU's databeskyttelsessystem. Betragtning 39 i GDPR beskriver dette princips afgørende funktion ved at anføre, at "*det bør være gennemsigtigt for de pågældende fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles, og i hvilket omfang personoplysningerne behandles eller vil blive behandlet. (...) Fysiske personer bør gøres bekendt med risici, regler, garantier og rettigheder i forbindelse med behandling af personoplysninger og med, hvordan de skal udøve deres rettigheder i forbindelse med en sådan behandling*."

80. Referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR nævner udtrykkeligt "gennemsigtighed" som et af de indholdsmæssige principper, der skal tages hensyn til ved vurderingen af, om et tredjelands beskyttelsesniveau i det væsentlige stemmer overens med niveauet i EU-retten. Nærmere bestemt anføres det, at "*alle fysiske personer skal underrettes om de vigtigste elementer i behandlingen af deres personoplysninger på en klar, lettilgængelig, kortfattet, gennemsigtig og letforståelig måde. Disse oplysninger skal omfatte formålet med behandlingen, den dataansvarliges identitet, de rettigheder, som den pågældende fysiske person har, samt andre oplysninger, der måtte være nødvendige af hensyn til rimeligheden. Der kan under visse omstændigheder være undtagelser fra denne ret til underretning, f.eks. af hensyn til efterforskning af strafbare handlinger, den nationale sikkerhed, retsvæsenets uafhængighed og retssager eller andre vigtige målsætninger af generel samfundsinteresse, som det er tilfældet i artikel 23 i GDPR.*"

81. Ligesom det er tilfældet med GDPR, gælder der i henhold til PIPA et generelt gennemsigtighedsprincip, der kræver, at persondataansvarlige offentliggør deres persondatapolitik og andre spørgsmål i forbindelse med behandling af personoplysninger (artikel 3, stk. 5, i PIPA). Der gælder særlige underretningskrav, når persondataansvarlige søger at indhente samtykke fra de registrerede til indsamling og behandling af personoplysninger (artikel 15, stk. 2, i PIPA), til videregivelse af personoplysninger til en tredjemand (artikel 17, stk. 2, i PIPA) og til behandling uden for formålet

[28] Som allerede fastsat i punkt 51-52 ovenfor og afsnit 3.1.1.1 i denne udtalelse.
[29] Se også afsnit 3.1.6 og 3.1.10 i denne udtalelse.

(artikel 18, stk. 3, i PIPA). Det skal bemærkes, at disse underretningsforpligtelser finder tilsvarende anvendelse på underleverandøren (artikel 26, stk. 7, i PIPA).

82. Databeskyttelsesrådet anerkender og bifalder de yderligere garantier i afsnit 3, nr. i) og ii), i underretning nr. 2021-1[30] vedrørende underretning af registrerede, når deres personoplysninger overføres af en EØS-enhed, idet det skal tages i betragtning, at der i henhold til artikel 20, stk. 1, i PIPA, når der ikke er indhentet oplysninger fra den registrerede, kun skal ske underretning af registrerede på anmodning, mens en generel ret til at blive underrettet kun anerkendes i henhold til artikel 20, stk. 2, i PIPA, hvis bestemte behandlingsaktiviteter overstiger de tærskler, der er fastsat i PIPA-gennemførelsesdekretet (artikel 15, stk. 2).

83. Databeskyttelsesrådet er generelt tilfreds med, at beskyttelsesniveauet i henhold til koreansk ret med hensyn til gennemsigtighedsprincippet i det væsentlige stemmer overens med niveauet i GDPR.

3.1.9. Særlige kategorier af personoplysninger

84. For at et tredjelands databeskyttelsessystem kan anerkendes som havende et beskyttelsesniveau for personoplysninger, der i det væsentlige stemmer overens med niveauet i GDPR, bør der findes særlige garantier, når der er tale om særlige kategorier af personoplysninger i den i artikel 9 og 10 i GDPR anvendte betydning.

85. I henhold til PIPA gælder der særlige bestemmelser for behandling af såkaldte følsomme oplysninger, som omfatter personoplysninger om ideologi, tro, optagelse i eller udtræden af en fagforening eller et politisk parti, politiske anskuelser, helbred, seksuelle forhold og andre personoplysninger, der kan forventes at udgøre en betydelig trussel mod privatlivets fred for en registreret, samt, under henvisning til PIPA-gennemførelsesdekretet, DNA-oplysninger, der er indsamlet ved genetiske test, personoplysninger, der udgør en straffeattest; personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende; og personoplysninger om race eller etnisk oprindelse.

86. I lighed med GDPR forbyder Koreas databeskyttelseslovgivning behandling af følsomme oplysninger, medmindre der gælder specifikke undtagelser, der består i 1) underretning af den registrerede og indhentning af et specifikt samtykke og 2) retlige bestemmelser, der tillader behandlingen (artikel 23, stk. 2, i PIPA).

87. På dette grundlag er Databeskyttelsesrådet i princippet enig i Europa-Kommissionens konklusion om, at Koreas lovgivning i det væsentlige stemmer overens med EU-lovgivningen, når det gælder behandling af særlige kategorier af personoplysninger. Databeskyttelsesrådet vil dog gerne bemærke, at det ikke har modtaget PIPA-håndbogen eller præciseringerne fra PIPC med hensyn til, at udtrykket "seksuelle forhold" fortolkes som også omfattende personens seksuelle orientering eller præferencer, som ikke er medtaget i underretning nr. 2021-1. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at fremlægge denne information for at kunne vurdere den uafhængigt. Endvidere opfordrer Databeskyttelsesrådet Europa-Kommissionen til specifikt at nævne de dokumenter, hvor den information, den henviser til om dette emne, kan findes.

3.1.10. Retten til indsigt, berigtigelse, sletning og indsigelse

88. Koreas retlige ramme anerkender registreredes rettigheder i henhold til artikel 3, stk. 5, i PIPA — i henhold til hvilken den persondataansvarlige skal garantere de rettigheder for registrerede, der er anført i artikel 4 i PIPA og nærmere angivet i artikel 35-37, 39 og artikel 39, stk. 2, i PIPA, og, hvad angår "kreditrelaterede personoplysninger" (dvs. "kreditoplysninger, nærmere bestemt oplysninger,

[30] Bilag I til udkastet til afgørelse.

der er nødvendige for at fastslå kreditværdigheden af parter i finansielle eller kommercielle transaktioner — se betragtning 3 i udkastet til afgørelse), i artikel 37, artikel 38 og artikel 38, stk. 3, i CIA.

89. Databeskyttelsesrådet bemærker, at retten til indsigt (og til berigtigelse og sletning, der kan udøves af en "*registreret, der har fået indsigt i sine personoplysninger i henhold til artikel 35*" i PIPA) kan begrænses eller nægtes, "*hvor indsigt forbydes eller begrænses ved love*", "*hvor indsigt kan forårsage skade på en tredjemands liv eller helbred eller uberettiget krænkelse af en anden persons ejendomsret og andre interesser*" og derudover, for offentlige institutioner, hvor det at give indsigt "*ville skabe alvorlige vanskeligheder*" for udøvelsen af bestemte funktioner, som nærmere angivet i artikel 35, stk. 4, i PIPA[31]. Tilsvarende bestemmelser findes i artikel 37 i PIPA vedrørende retten til suspension af behandling af personoplysninger.

90. Artikel 23 i GDPR giver EU-retten eller medlemsstaternes nationale ret mulighed for at begrænse individuelle rettigheder, når en sådan begrænsning respekterer kernen i de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund og omfatter sådanne begrænsninger for blandt andet at beskytte den registrerede eller andres rettigheder og frihedsrettigheder og "*kontrol-, tilsyns- eller reguleringsfunktioner, herunder funktioner af midlertidig karakter, der er forbundet med offentlig myndighedsudøvelse i de tilfælde, der er omhandlet i litra a)-e) og g), i samme artikel*".

91. På den baggrund ser Databeskyttelsesrådet gerne, at der i udkastet til afgørelse gives generel fornyet sikkerhed for behovet for, at enhver lov eller statut, der begrænser de registreredes rettigheder, opfylder kravene i Koreas forfatning om, at en grundlæggende rettighed kun kan begrænses, når det er nødvendigt af hensyn til den nationale sikkerhed eller opretholdelse af lov og orden eller den offentlige velfærd, og at denne begrænsning ikke må berøre kernen i den pågældende rettighed eller frihedsrettighed (artikel 37, stk. 2, i Koreas forfatning).

92. Med hensyn til undtagelsen vedrørende "*en uberettiget krænkelse af andre personers ejendom eller andre interesser*" anerkender Databeskyttelsesrådet endvidere, at dette "*indebærer, at der bør foretages en afvejning mellem personens forfatningsmæssigt beskyttede rettigheder og frihedsrettigheder på den ene side og andre personers rettigheder og frihedsrettigheder på den anden side*"[32], men det opfordrer Europa-Kommissionen til fuldt ud at overvåge anvendelsen af denne undtagelse og den relevante retspraksis med henblik på at sikre, at der også i praksis sikres et beskyttelsesniveau for registreredes rettigheder i Koreas retlige ramme, der i det væsentlige stemmer overens med niveauet i EU-retten.

93. På samme måde vil Databeskyttelsesrådet bifalde en omhyggelig overvågning af anvendelsen af undtagelsen for offentlige organer, navnlig med hensyn til de tilfælde, hvor det at give indsigt vil blive anset for at forårsage "*alvorlige vanskeligheder*" for udførelsen af deres opgaver, eftersom dette udtryk synes at være bredere end det, der anvendes i andre bestemmelser i PIPA, f.eks. i artikel 18, stk. 2, litra 5)[33], og bør fortolkes restriktivt for at undgå urimelige begrænsninger af registreredes rettigheder.

94. Databeskyttelsesrådet er desuden bekymret for, om undtagelserne, ifølge hvilke bestemmelserne vedrørende gennemsigtighed efter anmodning (artikel 20 i PIPA) og individuelle rettigheder (artikel

[31] De samme betingelser og undtagelser fra retten til indsigt og berigtigelse i henhold til PIPA gælder også med hensyn til retten til indsigt i og berigtigelse af kreditrelaterede personoplysninger i henhold til CIA (fodnote 135 i udkastet til afgørelse).

[32] Betragtning 76 i udkastet til afgørelse.

[33] For så vidt angår undtagelser fra begrænsningen til ikke-formålsbestemt anvendelse og afgivelse af personoplysninger, henviser artikel 18, stk. 2, litra 5), i PIPA til situationer, hvor det for offentlige institutioner "*er umuligt*" at udføre opgaverne.

35-37 i PIPA) – samt de tilsvarende bestemmelser vedrørende kravene til udbydere af informations- og kommunikationstjenester (artikel 39, stk. 2, og artikel 39, stk. 6-8, i PIPA) og bestemmelserne i CIA (jf. undtagelserne i artikel 40, stk. 3, i CIA) – ikke finder anvendelse, når det gælder pseudonymiserede personoplysninger, der behandles til statistiske formål, videnskabelige forskningsformål eller arkivformål i samfundets interesse (artikel 28, stk. 7, i PIPA), og er i overensstemmelse med garantierne i den europæiske retlige ramme.

95. Disse bestemmelser synes at indføre en generel undtagelse for denne form for behandling, mens GDPR fastsætter, at når personoplysninger (herunder pseudonymiserede personoplysninger) behandles til videnskabelige eller historiske forskningsformål eller statistiske formål, kan EU-retten eller medlemsstaternes nationale ret fastsætte undtagelser fra de registreredes rettigheder, men kun "*i det omfang sådanne rettigheder må forventes at gøre det umuligt eller i alvorlig grad hindre opfyldelsen af de specifikke formål, og sådanne undtagelser er nødvendige for at opfylde disse formål*", idet pseudonymisering kun er en af de tekniske og organisatoriske foranstaltninger, der kan iværksættes for at sikre, at princippet om dataminimering (artikel 89, stk. 1, i GDPR) overholdes.

96. Europa-Kommissionen mener, at undtagelsen i artikel 28, stk. 7, i PIPA er berettiget, også i lyset af artikel 28, stk. 5, i PIPA, hvori det udtrykkeligt forbydes den persondataansvarlige at behandle de pseudonymiserede personoplysninger med henblik på at identificere en bestemt person, og henviser til tilgangen i artikel 11, stk. 2, i GDPR (sammenholdt med betragtning 57 i GDPR) til behandling, der ikke kræver identifikation[34].

97. I henhold til artikel 11 i GDPR er den dataansvarlige ikke forpligtet til at "*beholde, indhente eller behandle yderligere oplysninger med henblik på at kunne identificere den registrerede*" alene med det formål at overholde GDPR, hvis formålene med den dataansvarliges behandling af personoplysninger ikke kræver eller ikke længere kræver, at den registrerede kan identificeres af den dataansvarlige; i sådanne tilfælde gælder vedkommendes rettigheder som registreret ikke, når den dataansvarlige kan påvise, at vedkommende ikke er i stand til at identificere den registrerede. Som anerkendt af Europa-Kommissionen[35] kræver GDPR derfor i sådanne tilfælde en "praktisk" umulighed for den dataansvarlige og anerkender i overensstemmelse med princippet om dataminimering, at det ikke er nødvendigt at behandle yderligere oplysninger "på grund af" GDPR.

98. Databeskyttelsesrådet anser imidlertid denne situation for at være forskellig fra den situation, hvor en dataansvarlig i praksis er i stand til at identificere den registrerede, men hvor det ikke er tilladt at gøre dette i henhold til en lovbestemmelse som den, der er indeholdt i artikel 28, stk. 5, i PIPA. I den forbindelse bifalder Databeskyttelsesrådet præciseringerne fra PIPC i underretning nr. 2021-1[36], som bekræfter, at afsnit 3 i PIPA (herunder artikel 28, stk. 7) og undtagelsen i artikel 40, stk. 3, i CIA kun finder anvendelse, når pseudonymiserede personoplysninger behandles til videnskabelige forskningsformål, statistiske formål eller arkivformål i samfundets interesse. Ud over de bekymringer, der allerede er nævnt med hensyn til den reelle bindende karakter af underretning nr. 2021-1[37] er Databeskyttelsesrådet imidlertid stadig i tvivl om, hvorvidt undtagelserne i artikel 28, stk. 7, i PIPA og artikel 40, stk. 3, i CIA kan betragtes som nødvendige og forholdsmæssige i et demokratisk samfund, for så vidt som de begrænser registreredes rettigheder i alle tilfælde, hvor pseudonymiserede

[34] Det skal bemærkes, at det samme ræsonnement ikke som sådan finder anvendelse på undtagelsen i artikel 40, stk. 3, i CIA for behandling af pseudonymiserede kreditoplysninger, fordi det i artikel 40, stk. 2, litra 6), er fastsat, at: "*Et kreditoplysningsfirma osv. må ikke behandle pseudonymiserede personoplysninger på en sådan måde, at en bestemt person kan identificeres med henblik på opnåelse af fortjeneste eller urimelige formål*", hvilket derfor kan give mulighed for fornyet identifikation til et rimeligt formål som forpligtelsen til at besvare en anmodning fra den registrerede.

[35] Jf. betragtning 82 i udkastet til afgørelse.

[36] Afsnit 4 i bilag I til udkastet til afgørelse.

[37] Jf. afsnit 3.1.1.1 ovenfor.

personoplysninger behandles til sådanne formål — dvs. selv om den persondataansvarlige i praksis er i stand til at identificere den registrerede, og rettighederne må forventes ikke at gøre det umuligt eller i alvorlig grad hindre opfyldelsen af de specifikke formål.

99. Databeskyttelsesrådet er navnlig bekymret for, at disse undtagelser ikke vil være berettigede og vil skulle undersøges nærmere, navnlig hvis de anvendes af den persondataansvarlige, der pseudonymiserer personoplysningerne "*til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse osv.*" i overensstemmelse med artikel 28, stk. 2, i PIPA "*uden de registreredes samtykke*" (og uden at foretage underretning som omhandlet i artikel 20 i PIPA)[38], for så vidt som denne persondataansvarlige beholder de personoplysninger, der gør det muligt at foretage en fornyet identifikation. I henhold til GDPR bør fysiske personer kunne udøve deres rettigheder med hensyn til oplysninger, som kan identificere eller udpege dem, selv om oplysningerne betragtes som "pseudonymiserede", medmindre den allerede nævnte artikel 11 i GDPR finder anvendelse. I den forbindelse bemærker Databeskyttelsesrådet, at kun når disse oplysninger videregives til en tredjemand til de samme statistiske formål, videnskabelige forskningsformål og arkivformål, bør oplysninger, der kan anvendes til at identificere en bestemt person, ikke medtages, og derfor vil kun den persondataansvarlige, til hvem pseudonymiserede personoplysninger videregives i henhold til artikel 28-2, stk. 2, i PIPA, sandsynligvis "i praksis" ikke være i stand til at identificere den registrerede uden yderligere oplysninger.

100. I betragtning af, at PIPA, som anerkendt af Europa-Kommissionen, "*i stedet for at gøre brug af pseudonymisering som en mulig garanti kræver pseudonymisering som en forudsætning for at udføre visse behandlingsaktiviteter til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse (f.eks. for at kunne behandle oplysningerne uden samtykke eller kombinere forskellige datasæt)*"[39] – men i sådanne tilfælde fastsætter PIPA væsentlige begrænsninger af de registreredes rettigheder –, opfordrer Databeskyttelsesrådet Europa-Kommissionen til at foretage en nærmere vurdering af undtagelserne i artikel 28, stk. 7, i PIPA og artikel 40, stk. 3, i CIA og til omhyggeligt at overvåge disses anvendelse og den relevante retspraksis[40] med henblik på at sikre, at de registreredes rettigheder ikke begrænses i urimelig grad, når personoplysninger, der overføres i henhold til afgørelsen om et tilstrækkeligt beskyttelsesniveau, behandles til disse formål, under hensyntagen til at disse rettigheder i mange tilfælde også hjælper den dataansvarlige til at sikre de behandlede datas kvalitet.

3.1.11. Begrænsninger for videreoverførsel

101. I referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR præciseres det, at beskyttelsesniveauet for fysiske personer, hvis personoplysninger overføres i henhold til en afgørelse om et tilstrækkeligt beskyttelsesniveau, ikke må undermineres af videreoverførslen, og at videreoverførsel derfor "*kun bør være tilladt, når den efterfølgende modtager (dvs. modtageren af videreoverførslen) også er underlagt regler (herunder kontraktbestemmelser), som giver et tilstrækkeligt beskyttelsesniveau, og følger de relevante instrukser ved behandling af personoplysninger på den dataansvarliges vegne*".

102. Hvad angår videreoverførsel til underleverandører (dvs. "databehandlere"), der er etableret i andre tredjelande, noterer Databeskyttelsesrådet sig, at der ikke findes særlige regler i Koreas retlige ramme

[38] Se artikel 27, stk. 7, i PIPA, som beskrevet i underretning nr. 2021-1, hvorefter visse garantier i PIPA, dvs. "*artikel 20, 21, 27, artikel 34, stk. 1, artikel 35-37, artikel 39, stk. 3-4, og artikel 39, stk. 6-8)*", ikke finder anvendelse på pseudonymiserede personoplysninger, der behandles med henblik på at udarbejde statistikker, drive videnskabelig forskning, opbevare offentlige registre osv.
[39] Betragtning 42 i udkastet til afgørelse.
[40] Jf. f.eks. Open Nets forfatningsmæssige udfordringer (information https://opennet.or.kr/19909 findes kun på koreansk).

til at dække disse tilfælde, og at en koreansk persondataansvarlig som vurderet af Europa-Kommissionen[41] skal sikre overholdelse af PIPA's bestemmelser om outsourcing (artikel 26 i PIPA) ved hjælp af et juridisk bindende instrument, og at den persondataansvarlige vil være ansvarlig for de personoplysninger, der er blevet outsourcet (artikel 26 i PIPA).

103. Med hensyn til videreoverførsel til tredjemand (dvs. andre persondataansvarlige) skal en koreansk persondataansvarlig i henhold til artikel 17, stk. 3, i PIPA underrette de registrerede om og indhente deres samtykke til de grænseoverskridende overførsler, og den persondataansvarlige "*må ikke indgå en kontrakt om grænseoverskridende overførsel af personoplysninger i strid med PIPA*". Databeskyttelsesrådet bemærker, at denne sidste bestemmelse — som Europa-Kommissionen har taget stilling til[42] —, vil sikre, at ingen kontrakt om grænseoverskridende overførsler kan indeholde forpligtelser, der er i modstrid med de krav, som PIPA pålægger den persondataansvarlige, og derfor kan betragtes som en garanti, men den pålægger ingen forpligtelse til at indføre garantier, der sikrer, at modtageren yder samme beskyttelsesniveau som PIPA. Databeskyttelsesrådet anerkender derfor, at informeret samtykke fra den registrerede generelt vil blive anvendt som grundlag for dataoverførsler fra en persondataansvarlig, der er etableret i Korea, til en modtager, der er etableret i et tredjeland.

104. I den forbindelse bifaldes PIPC's yderligere præciseringer i underretning nr. 2021-1 vedrørende forpligtelsen til at underrette fysiske personer om det tredjeland, som deres oplysninger vil blive videregivet til[43], da dette — som fremhævet af Europa-Kommissionen[44] — vil hjælpe registrerede i EØS med at træffe en velfunderet beslutning om, hvorvidt de vil give deres samtykke til en udenlandsk bestemmelse.

105. Som det også er tilfældet i udtalelse 28/2018 om Europa-Kommissionens udkast til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger i Japan, skal det understreges, at registrerede i henhold til GDPR forud for samtykke udtrykkeligt skal underrettes om de mulige risici ved sådanne overførsler som følge af manglende tilstrækkelig beskyttelse i tredjelandet og manglen på fornødne garantier. En sådan underretning bør f.eks. indeholde information om, at der i tredjelandet muligvis ikke findes en tilsynsmyndighed og/eller databehandlingsprincipper, og/eller at den registreredes rettigheder måske slet ikke er tilgodeset i tredjelandet[45]. For Databeskyttelsesrådet er det afgørende at give denne information for at gøre det muligt for den registrerede at give informeret samtykke under fuldt kendskab til de specifikke forhold i forbindelse med overførslen[46]. Databeskyttelsesrådet er derfor bekymret over Europa-Kommissionens konklusioner i udkastet til afgørelse om et tilstrækkeligt beskyttelsesniveau med hensyn til denne specifikke form for overførsler. Registrerede har normalt ikke kendskab til rammen for databeskyttelse i tredjelande. Det kan derfor ikke konkluderes, at en registreret kan vurdere risikoen ved en overførsel ved kun at kende det specifikke bestemmelsesland. Der skal derimod foreligge klar information om de specifikke risici ved en sådan overførsel af personoplysninger til et land uden for Republikken Koreas område forud for den registreredes samtykke.

106. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at sikre, at underretningen af den registrerede om "*omstændighederne ved overførslen*" også omfatter information om de mulige risici ved overførslen som følge af manglende tilstrækkelig beskyttelse i tredjelandet samt manglen på

[41] Betragtning 87 i udkastet til afgørelse.
[42] Betragtning 88 i udkastet til afgørelse.
[43] Ibid.
[44] Ibid.
[45] Det Europæiske Databeskyttelsesråds retningslinjer 2/2018 om undtagelser i artikel 49 i forordning 2016/679, 25. maj 2018, s. 8.
[46] Det Europæiske Databeskyttelsesråds retningslinjer 2/2018 om undtagelser i artikel 49 i forordning 2016/679, 25. maj 2018, s. 7.

fornødne garantier. Dette er vigtigt for Databeskyttelsesrådet af hensyn til vurderingen af, om samtykkekravene i det væsentlige stemmer overens med kravene i GDPR.

107. I betragtning af at samtykke skal gives frit, hvile på et informeret grundlag samt være specifikt og utvetydigt, ser Databeskyttelsesrådet desuden gerne, at der i afgørelsen om et tilstrækkeligt beskyttelsesniveau gives fornyet sikkerhed for, at personoplysninger ikke vil blive overført fra koreanske persondataansvarlige til et tredjeland i en situation, hvor et gyldigt samtykke i henhold til GDPR ikke kan gives, f.eks. på grund af en ulige magtbalance.

108. I forbindelse med tilfælde, hvor den persondataansvarlige kan videregive personoplysninger til en tredjemand i udlandet uden den registreredes samtykke — dvs. 1) hvis personoplysninger videregives inden for de rammer, der med rimelighed kan henføres til det oprindelige formål med indsamlingen i henhold til artikel 17, stk. 4, i PIPA, og 2) hvis personoplysninger kan videregives til en tredjemand i ekstraordinære tilfælde som omhandlet i artikel 18, stk. 2, i PIPA — noterer Databeskyttelsesrådet sig PIPC's præciseringer i afsnit 2 i underretning nr. 2021-1 (og bifalder den planlagte forpligtelse, der pålægges den i Korea etablerede dataansvarlige og den udenlandske modtager til gennem et juridisk bindende instrument (f.eks. en kontrakt) at sikre et beskyttelsesniveau, der stemmer overens med PIPA, herunder når det gælder registreredes rettigheder).

3.1.12. Direkte markedsføring

109. I henhold til artikel 21, stk. 2, og artikel 21, stk. 3, i GDPR og referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR skal den registrerede altid uden omkostninger kunne gøre indsigelse mod databehandling, der finder sted med henblik på profilering og direkte markedsføring.

110. Med hensyn til retten til suspension i henhold til artikel 37 i PIPA anerkender Databeskyttelsesrådet, at Europa-Kommissionen mener, at denne ret også gælder, når data anvendes med henblik på direkte markedsføring[47]. Databeskyttelsesrådet ser dog gerne, at der anføres yderligere information og præciseringer i udkastet til afgørelse i forbindelse med denne vurdering og navnlig vedrørende den praktiske anvendelse af retten til suspension i forbindelse med direkte markedsføring (f.eks. henvisninger til relevant retspraksis osv.). I den forbindelse fremhæver Databeskyttelsesrådet også, at retten til at anmode en udbyder/bruger af kreditoplysninger om at ophøre med at kontakte vedkommende for at præsentere eller opfordre til køb af varer eller tjenesteydelser er udtrykkeligt fastsat i CIA (artikel 37, stk. 2).

111. Som anerkendt af Europa-Kommissionen[48] kræver en sådan behandling i henhold til Koreas retlige ramme desuden generelt et specifikt (supplerende) samtykke fra den registrerede (jf. artikel 15, stk. 1, litra 1), artikel 17, stk. 2, litra 1), i PIPA).

112. Da det ikke kan udelukkes, at personoplysninger, der overføres fra EØS, kan behandles i Korea til sådanne formål, ser Databeskyttelsesrådet også gerne, at der indføres præciseringer i afgørelsen om et tilstrækkeligt beskyttelsesniveau vedrørende eksistensen af den registreredes ret til at trække sit samtykke tilbage[49] og retten til at få sine personoplysninger slettet og ikke længere behandlet, hvis behandlingen er baseret på samtykke (f.eks. i forbindelse med behandling med henblik på markedsføring), og den registrerede har trukket sit samtykke tilbage.

[47] Betragtning 79 i udkastet til afgørelse.
[48] Ibid.
[49] Se også ovenfor under punkt 67: Selv om muligheden for at tilbagekalde samtykke er tydeligt omhandlet i artikel 37, stk. 1, i CIA, nævnes denne ret kun to gange i PIPA i forbindelse med specifikke omstændigheder i artikel 27, stk. 1, litra 2), og artikel 39, stk. 7.

3.1.13. Automatiske afgørelser og profilering

113. Som anerkendt af Europa-Kommissionen i sit udkast til afgørelse[50] indeholder PIPA og dens gennemførelsesdekret ikke generelle bestemmelser om spørgsmålet om afgørelser, der berører den registrerede, og som udelukkende er baseret på automatisk behandling af personoplysninger. Det koreanske retssystem lægger dog op til en sådan ret i CIA, som indeholder regler om automatiske afgørelser (artikel 36, stk. 2), selv om anvendelsen af dem synes at ligge uden for anvendelsesområdet for PIPC's tilsyn (og som sådan uden for anvendelsesområdet for dette udkast til afgørelse — jf. afsnit 2.3.2 ovenfor om anvendelsesområdet for udkastet til afgørelse).

114. Som allerede fastslået af henholdsvis artikel 29-Gruppen[51] i dennes udtalelse 1/2016 om privatlivsskjold og Databeskyttelsesrådet i dettes tidligere udtalelse om afgørelsen om et tilstrækkeligt beskyttelsesniveau vedrørende Japan[52], peger den stigende betydning af automatiske afgørelser, profilering og kunstig intelligens mod at anlægge en mere beskyttende tilgang i denne henseende. I modsætning til Europa-Kommissionens argumenter[53] om, at det er usandsynligt, at manglen på specifikke regler om automatiske afgørelser i PIPA vil påvirke beskyttelsesniveauet for personoplysninger, der er indsamlet i Unionen (eftersom enhver afgørelse, der er baseret på automatisk behandling, typisk vil blive truffet af den dataansvarlige i Unionen, som har en direkte forbindelse med den pågældende registrerede), mener Databeskyttelsesrådet ikke, at det kan udelukkes, at en persondataansvarlig, der er etableret i Korea, kan anvende automatiske afgørelser i forbindelse med personoplysninger, der overføres i henhold til afgørelsen om et tilstrækkeligt beskyttelsesniveau (f.eks. i forbindelse med ansættelse, til vurdering af arbejdsresultater, pålidelighed, adfærd osv.).

115. Udvikling af nye teknologier gør det lettere for virksomheder at indføre eller overveje at indføre systemer til automatiske afgørelser, hvilket kan medføre en forringelse af fysiske personers stilling. Når afgørelser, der udelukkende træffes af automatiske systemer, har konsekvenser for fysiske personers retsstilling eller i væsentlig grad påvirker dem (f.eks. ved sortlistning og dermed fratagelse af fysiske personers rettigheder), er det afgørende at sikre tilstrækkelige garantier, herunder retten til at blive underrettet om de specifikke årsager til afgørelsen og logikken deri, at berigtige urigtige eller ufuldstændige oplysninger og at anfægte afgørelsen, hvis den er truffet på et forkert faktuelt grundlag.[54]

116. I den forbindelse er Databeskyttelsesrådet bekymret over manglen på retlige bestemmelser om automatiske afgørelser i PIPA og opfordrer derfor Europa-Kommissionen til at se på dette punkt og fortsat overvåge udviklingen af Koreas retlige ramme i denne henseende.

3.1.14. Ansvarlighed

117. Koreas retlige ramme indeholder en række regler, der har til formål at sikre, at persondataansvarlige træffer passende tekniske og organisatoriske foranstaltninger til effektivt at opfylde deres databeskyttelsesmæssige forpligtelser og kan påvise en sådan overholdelse, blandt andet over for den kompetente tilsynsmyndighed. Databeskyttelsesrådet bifalder navnlig, at der findes regler om vedtagelse af en intern forvaltningsplan (artikel 29 i PIPA), en forpligtelse til at gennemføre en såkaldt

[50] Jf. betragtning 81 i udkastet til afgørelse.

[51] Denne arbejdsgruppe blev nedsat ved artikel 29 i direktiv 95/46/EF. Den var et uafhængigt europæisk rådgivende organ for beskyttelse af personoplysninger og privatlivets fred. Dens opgaver er beskrevet i artikel 30 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF. Artikel 29-Gruppen er nu blevet til Databeskyttelsesrådet.

[52] Udtalelse 28/2018 om Europa-Kommissionens udkast til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger i Japan, vedtaget den 5. december 2018.

[53] Betragtning 81 i udkastet til afgørelse.

[54] WP 254, s. 7.

konsekvensanalyse vedrørende beskyttelse af privatlivets fred ("**PIA**") i tilfælde, hvor behandlingen udgør en højere risiko for mulige krænkelser af privatlivets fred (artikel 33, stk. 1, i PIPA og artikel 35 i PIPA-gennemførelsesdekretet), regler om uddannelse af og tilsyn med ansatte (artikel 28 i PIPA) samt en forpligtelse til at udpege en databeskyttelsesrådgiver (artikel 31 i PIPA sammenholdt med artikel 32 i PIPA-gennemførelsesdekretet).

118. Databeskyttelsesrådet deler Europa-Kommissionens opfattelse vedrørende den i det væsentlige overensstemmende beskyttelse, som reglerne sikrer — selv i tilfælde, hvor reglerne synes at afvige relativt fra reglerne i GDPR, f.eks. er der ingen bestemmelse om, at databeskyttelsesrådgiveren skal være uafhængig, men det er klart fastsat, at den pågældende skal referere til den persondataansvarliges ledelse (artikel 31, stk. 4, i PIPA), og at den pågældende ikke må udsættes for uberettigede ulemper som følge af udførelsen af disse funktioner (artikel 31, stk. 5, i PIPA) — og vil foreslå, at Europa-Kommissionen i forbindelse med vurderingen af afgørelsen om et tilstrækkeligt beskyttelsesniveau overvåger den faktiske anvendelse af disse bestemmelser med henblik på at vurdere deres faktiske gennemførelse.

3.2. Procedure- og håndhævelsesmekanismer

119. På grundlag af kriterierne i referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR har Databeskyttelsesrådet analyseret følgende aspekter af Koreas ramme for databeskyttelse, som er omfattet af udkastet til afgørelse: eksistensen af en uafhængig tilsynsmyndighed, der fungerer effektivt; eksistensen af et system, der sikrer en høj grad af overholdelse og et system med adgang til passende klage- og søgsmålsmekanismer, der giver EØS-borgere mulighed for at gøre deres rettigheder gældende og opnå adgang til administrativ og retslig prøvelse uden hindringer.

120. I henhold til kapitel VI i GDPR og kapitel 3 i referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR skal der være en eller flere uafhængige tilsynsmyndigheder, der har til opgave at overvåge, sikre og håndhæve overholdelsen af bestemmelserne om databeskyttelse og beskyttelse af privatlivets fred i tredjelandet for at sikre overensstemmelse med beskyttelsesniveauet i EØS.

121. Tilsynsmyndigheden skal handle fuldstændig uafhængigt og uvildigt ved udførelsen af sine opgaver og udøvelsen af sine beføjelser og skal hverken indhente eller modtage instrukser. Desuden skal tilsynsmyndigheden have alle tilgængelige beføjelser og hverv, der er nødvendige for at sikre, at databeskyttelsesrettighederne overholdes, og øge kendskabet til disse. Der bør endvidere tages hensyn til tilsynsmyndighedens ansatte og budget. Tilsynsmyndigheden skal også kunne iværksætte foranstaltninger på eget initiativ.

3.2.1. Kompetent uafhængig tilsynsmyndighed

122. I Republikken Korea er PIPC den uafhængige myndighed med ansvar for overvågning og håndhævelse af PIPA. PIPC er sammensat af en formand, en næstformand og syv kommissionsmedlemmer. Formanden og næstformanden udnævnes af præsidenten efter indstilling fra premierministeren. To af kommissionsmedlemmerne udnævnes efter indstilling fra formanden, to efter indstilling fra repræsentanter for det politiske parti, som præsidenten tilhører, og de tre øvrige medlemmer efter indstilling fra repræsentanter for andre politiske partier (artikel 7, stk. 2, litra 2), i PIPA). PIPC bistås af et sekretariat (artikel 7, stk. 13) og kan nedsætte underudvalg (bestående af tre kommissionsmedlemmer) til at behandle mindre overtrædelser og tilbagevendende sager (artikel 7, stk. 12, i PIPA).

123. I den henseende anerkender Databeskyttelsesrådet, at PIPC trods sin nylige omstrukturering, som ændrede kommissionens status og beføjelser gennemgribende, har gjort en betydelig indsats for at opbygge den infrastruktur, der er nødvendig for at muliggøre gennemførelsen af PIPA og de seneste ændringer hertil. Blandt bestræbelserne kan nævnes udarbejdelse af PIPC's regler, udarbejdelse af retningslinjer for fortolkning af PIPA og oprettelse af en hjælpetjeneste til at rådgive erhvervsdrivende og fysiske personer om databeskyttelsesbestemmelser samt en mæglingstjeneste til at behandle

klager. PIPC's opgaver omfatter navnlig rådgivning om love og bestemmelser vedrørende databeskyttelse, udvikling af databeskyttelsespolitikker og -retningslinjer, undersøgelse af krænkelser af individuelle rettigheder, behandling af klager og mægling i tvister, håndhævelse af overholdelse af PIPA, tilvejebringelse af uddannelse og information på databeskyttelsesområdet samt udveksling og samarbejde med tredjelandes databeskyttelsesmyndigheder.[55]

124. Udnævnelsen af medlemmerne af PIPC og sammensætningen heraf er reguleret i artikel 7, stk. 2, i PIPA. Selv om PIPC hører under premierministerens kompetence (og formanden og næstformanden udnævnes af præsidenten efter indstilling fra premierministeren), indeholder de retlige rammer krav om, at kommissionsmedlemmerne udfører deres opgaver uafhængigt i henhold til loven og deres samvittighed. Databeskyttelsesrådet anerkender de institutionelle og proceduremæssige garantier, der er indeholdt i PIPA, og navnlig i artikel 7, stk. 4-7. Databeskyttelsesrådet ser dog gerne, at Europa-Kommissionen overvåger enhver udvikling, der kan påvirke uafhængigheden hos medlemmerne af den sydkoreanske tilsynsmyndighed.

125. Desuden indeholder udkastet til afgørelse endnu ikke en analyse af PIPC's budget, herunder finansieringskilder og budgetgennemsigtighed. Databeskyttelsesrådet finder, at dette element, der er nævnt i både artikel 56, stk. 1, i GDPR og de proceduremæssige og håndhævelsesmæssige databeskyttelsesprincipper og -mekanismer, der skal tages hensyn til i henhold til referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR i forbindelse med evalueringen af et lands eller en international organisations system, skal tages grundigt i betragtning, da det er en indikator for de økonomiske og menneskelige ressourcer, som tilsynsmyndigheden har til rådighed til at opfylde sine lovbestemte forpligtelser og opgaver på databeskyttelsesområdet uafhængigt, og råder derfor Europa-Kommissionen til at redegøre nærmere for dette i udkastet til afgørelse.

3.2.2. Eksistensen af et databeskyttelsessystem, der sikrer en høj grad af overholdelse

126. På håndhævelsesområdet anerkender Databeskyttelsesrådet PIPC's forskellige håndhævelsesmæssige beføjelser og sanktioner som fastsat i PIPA og CIA og noterer sig præciseringerne i underretning nr. 2021-1 om, at betingelserne i artikel 64, stk. 1, i PIPA og artikel 45, stk. 4, i CIA[56] vil finde anvendelse, når der handles i strid med de principper, rettigheder og forpligtelser i lovgivningen, der beskytter personoplysninger. Databeskyttelsesrådet anbefaler dog, at Europa-Kommissionen omhyggeligt overvåger anvendelsen i praksis af PIPC's beføjelser til at pålægge den part, der handler i strid med principperne, rettighederne og forpligtelserne, at træffe de foranstaltninger, som den anser for passende blandt foranstaltningerne i artikel 64, stk. 1, eller artikel 45, stk. 4, i CIA.

127. Hvad angår de korrigerende foranstaltninger i artikel 64, stk. 1, i PIPA, har PIPC i tilfælde af manglende overholdelse af en korrigerende foranstaltning beføjelse til at pålægge en bøde på højst 50 mio. sydkoreanske won (artikel 75, stk. 2, litra 13), i PIPA). Beløbet svarer til 36 564 EUR. Databeskyttelsesrådet er af den opfattelse og er bekymret for, at et så begrænset omfang af bøder muligvis ikke har nogen tilstrækkeligt afskrækkende virkning på overtrædere som tilsigtet med loven med henblik på at sikre håndhævelsen af databeskyttelsesreglerne, da bøderne ikke synes at være tilstrækkelige som afskrækningsmiddel, især ikke for store organisationer eller virksomheder med betydelige finansielle ressourcer.

128. Med hensyn til muligheden for, at PIPC kan kræve, at lederen af et centralt administrativt organ efterforsker den persondataansvarlige eller deltager i en efterforskning af overtrædelser af PIPA og

[55] PIPC's opgaver og beføjelser er hovedsagelig fastsat i artikel 7, stk. 8, og artikel 7, stk. 9, samt i artikel 61-66 i PIPA.

[56] Dvs."*en overtrædelse af loven anses for at kunne forventes at krænke fysiske personers rettigheder og frihedsrettigheder med hensyn til personoplysninger, og hvis der ikke gribes ind, er der sandsynlighed for, at dette vil medføre skader, som det er vanskeligt at afhjælpe*".

endda pålægger korrigerende foranstaltninger, for så vidt angår persondataansvarlige under deres jurisdiktion (artikel 63, stk. 4-5, i PIPA), bemærker Databeskyttelsesrådet, at selv om der er givet en vis information i betragtning 122 i udkastet til afgørelse, er disse andre organers karakter og deres juridiske forbindelser med PIPC stadig generelt temmelig uklare. Desuden henvises der i artikel 68, stk. 1, i PIPA til mange enheder, som det vil være muligt at uddelegere PIPC's beføjelser til. Selv om det ser ud til, at denne bestemmelse kun er blevet anvendt i forbindelse med Koreas internet- og sikkerhedsmyndighed[57], vil Databeskyttelsesrådet bifalde præciseringer med hensyn til karakteren af de mulige interaktioner mellem disse enheder samt omhyggelig overvågning af anvendelsen af denne bestemmelse i fremtiden med henblik på at sikre uafhængigheden af de enheder, der har til opgave at bringe databeskyttelsesreglerne i anvendelse.

129. Med hensyn til sanktioner synes det koreanske system at kombinere forskellige typer sanktioner, fra korrigerende foranstaltninger og administrative bøder til strafferetlige sanktioner, som må forventes at have en stærk afskrækkende virkning, og de koreanske myndigheder fremlagde en række eksempler på bøder, som PIPC for nylig har pålagt, blandt andet en bøde på 6,7 mia. sydkoreanske won til en virksomhed i december 2020 for overtrædelse af en række bestemmelser i PIPA, og en anden bøde på 103,3 mio. sydkoreanske won den 28. april 2021 til en teknologivirksomhed inden for kunstig intelligens for overtrædelse af reglerne om lovlig behandling, navnlig samtykke, og behandling af pseudonymiserede personoplysninger.

130. Selv om de nævnte beløb kan have en afskrækkende virkning, vil Databeskyttelsesrådet bifalde at modtage yderligere information om den metode, som PIPC anvender til at beregne niveauet for administrative bøder, f.eks. med hensyn til bøder, der pålægges for manglende overholdelse af en korrigerende foranstaltning, der er iværksat i henhold til artikel 64, stk. 1, i PIPA (jf. artikel 75, stk. 2, litra 13), i PIPA). Dette er især relevant i forbindelse med strafferetlige sanktioner og anvendelsen af den (koreanske) straffelov.

3.2.3. Databeskyttelsessystemet skal støtte og hjælpe de registrerede med at udøve deres rettigheder og omfatte passende klage- og søgsmålsmekanismer

131. Hvad angår adgang til administrativ og retslig prøvelse, synes det koreanske system at tilbyde forskellige muligheder for at sikre tilstrækkelig beskyttelse og navnlig håndhævelse af individuelle rettigheder med adgang til effektiv administrativ og retslig prøvelse, herunder krav om erstatning for skader

132. Det koreanske system tilbyder også alternative mekanismer, som fysiske personer kan gøre brug af, ud over adgang til administrativ og retslig prøvelse, som beskrevet i betragtning 132 og 133 i udkastet til afgørelse, nærmere bestemt et callcenter på databeskyttelsesområdet (Privacy Call Centre) og et udvalg for mægling i tvister (Dispute Mediation Committee). Da der er tale om supplerende klagemuligheder, vil Databeskyttelsesrådet bifalde at modtage en nærmere redegørelse for, hvordan de supplerer klage- og søgsmålsmulighederne ved PIPC og domstolene for registrerede, hvis personoplysninger overføres til Korea i henhold til afgørelsen om et tilstrækkeligt beskyttelsesniveau.

4. SYDKOREANSKE OFFENTLIGE MYNDIGHEDERS INDSIGT I OG ANVENDELSE AF PERSONOPLYSNINGER OVERFØRT FRA DEN EUROPÆISKE UNION

133. Med hensyn til vurderingen af databeskyttelsesniveauet på områderne retshåndhævelse og national sikkerhed fremlagde Europa-Kommissionen omfattende information i sit udkast til afgørelse og de

[57] Jf. betragtning 117 i udkastet til afgørelse og artikel 62 i gennemførelsesdekretet.

bilag, der blev stillet til rådighed. Databeskyttelsesrådet undlader derfor at gengive hovedparten af de faktuelle informationer og vurderinger i denne udtalelse.

134. Europa-Kommissionen konkluderer, at databeskyttelsesniveauet på ovennævnte områder stemmer overens med de krav, der fremgår af Domstolens retspraksis, og som derfor kan anses for i det væsentlige at stemme overens med niveauet i Den Europæiske Union.

135. Som en generel bemærkning vil Databeskyttelsesrådet gerne understrege, at selv i tilfælde, hvor det ser ud til eller forventes af Europa-Kommissionen, at personoplysninger, der overføres fra EU til Sydkorea, ikke vil blive berørt af den relevante koreanske lovgivning, er det stadig på sin plads at vurdere, om det koreanske databeskyttelsesniveau er tilstrækkeligt i sådanne tilfælde. Disse tilfældes relevans fremgår også af, at Europa-Kommissionen selv har behandlet dem i udkastet til afgørelse.

4.1. Generel ramme for databeskyttelse i forbindelse med offentlige myndigheders indsigt

136. Hvad angår offentlige myndigheders indsigt i personoplysninger, er det nødvendigt at se nærmere på en række koreanske love for at vurdere beskyttelsesniveauet for retten til privatlivets fred og beskyttelse af personoplysninger. For det første bemærker Databeskyttelsesrådet, at PIPA som en central databeskyttelseslov angiveligt finder bred anvendelse. Men selv om PIPA finder fuld anvendelse på retshåndhævelsesområdet, er dens anvendelse på databehandling, der finder sted af hensyn til den nationale sikkerhed, begrænset. I henhold til artikel 58, stk. 1, litra 2), i PIPA finder kapitel III-VII ikke anvendelse på behandling af personoplysninger, der finder sted af hensyn til den nationale sikkerhed. Kapitel I, II, IX og X finder dog fortsat anvendelse på området national sikkerhed. PIPA's centrale principper samt de grundlæggende garantier for registreredes rettigheder og bestemmelserne om tilsyn, håndhævelse og retsmidler finder således anvendelse på nationale sikkerhedsmyndigheders indsigt i og anvendelse af personoplysninger.

137. Sydkoreas forfatning indeholder også væsentlige databeskyttelsesprincipper, nærmere bestemt legalitetsprincippet, nødvendighedsprincippet og proportionalitetsprincippet. [58]Disse principper finder også anvendelse på sydkoreanske offentlige myndigheders indsigt i personoplysninger på områderne retshåndhævelse og national sikkerhed.

138. På retshåndhævelsesområdet kan politi, anklagere, domstole og andre offentlige myndigheder indsamle personoplysninger på grundlag af specifik lovgivning, dvs. strafferetsplejeloven ("**CPA**"), loven om beskyttelse af personoplysninger i forbindelse med kommunikation ("**CPPA**"), loven om telekommunikationsvirksomhed ("**TBA**") og loven om indberetning og anvendelse af specifikke finansielle transaktionsoplysninger ("**ARUSFTI**"), som finder anvendelse på retsforfølgelse og forebyggelse af hvidvask og finansiering af terrorisme. Disse specifikke love fastsætter yderligere begrænsninger, garantier og undtagelser.

139. På området national sikkerhed kan den nationale efterretningstjeneste ("**NIS**") indsamle personoplysninger og aflytte kommunikation på grundlag af loven om den nationale sikkerhedstjeneste ("**NISA**") og yderligere "love vedrørende den nationale sikkerhed"[59]. Databeskyttelsesrådet har erfaret, at NIS ved udøvelsen af sine beføjelser skal overholde ovennævnte retlige bestemmelser samt PIPA.

[58] Jf. betragtning 145 i udkastet til afgørelse.

[59] Lovene vedrørende den nationale sikkerhed omfatter blandt andet loven om beskyttelse af personoplysninger i forbindelse med kommunikation, loven om bekæmpelse af terrorisme til beskyttelse af borgerne og den offentlige sikkerhed og loven om telekommunikationsvirksomheder.

140. Databeskyttelsesrådet anmoder Kommissionen om at præcisere, om der ud over NIS er andre myndigheder i Korea, der er ansvarlige for området national sikkerhed, da Europa-Kommissionen i bilag I, afsnit 6, giver indtryk af NIS som et eksempel på en national sikkerhedsmyndighed.

4.2. Beskyttelse af og garantier for kommunikationsbekræftelsesdata i forbindelse med offentlige myndigheders indsigt med henblik på retshåndhævelse

141. På grundlag af den relevante lov, CPPA, kan retshåndhævende myndigheder træffe to typer foranstaltninger for at få indsigt i kommunikationsoplysninger. CPPA skelner mellem kommunikationsbegrænsende foranstaltninger, der omfatter både indsamling af indhold i almindelig post og direkte aflytning af indhold i telekommunikation[60], og indsamling af såkaldte kommunikationsbekræftelsesdata. Sidstnævnte omfatter datoen for telekommunikation, start- og sluttidspunkt, antal udgående og indgående opkald samt den anden parts abonnentnummer, anvendelseshyppighed, logfiler om brugen af telekommunikationstjenester og lokaliseringsoplysninger.[61]

142. Databeskyttelsesrådet bemærker, at kommunikationsbekræftelsesdata ikke synes at nyde godt af de samme garantier som data, der indsamles via kommunikationsbegrænsende foranstaltninger, dvs. indholdsdata. Databeskyttelsesrådet bemærker også, at indsamlingen af indhold er omfattet af flere garantier end indsamlingen af kommunikationsbekræftelsesdata med henblik på retshåndhævelse: For det første er indsamlingen af kommunikationsbekræftelsesdata, i modsætning til indsamlingen af indholdsdata, ikke begrænset til efterforskning af bestemte alvorlige forbrydelser, men kan foretages, når det skønnes nødvendigt for at gennemføre "enhver efterforskning eller fuldbyrde en straf" (artikel 13, stk. 1, i CPPA). For det andet er indsamlingen af kommunikationsbekræftelsesdata i princippet ikke struktureret som en sidste udvej og må kun anvendes, hvis det er vanskeligt på anden måde at forhindre, at der begås en forbrydelse, anholde den kriminelle eller indsamle bevismateriale[62]. Kommunikationsbekræftelsesdata kan indsamles, når en anklager eller en kriminalbetjent "finder det nødvendigt" for at efterforske en forbrydelse eller fuldbyrde en straf. Der findes dog en undtagelse i denne henseende for realtidsbaserede sporingsdata og kommunikationsbekræftelsesdata vedrørende en specifik basisstation i henhold til artikel 13, stk. 2, i CPPA. For det tredje skal retshåndhævende myndigheder, der indsamler indholdet af kommunikation, straks ophøre hermed, når fortsat indsigt ikke længere anses for nødvendig.[63] Hvad angår kommunikationsbekræftelsesdata, er dette i hvert fald ikke udtrykkeligt fastsat i CPPA eller dens gennemførelsesdekret.

143. Databeskyttelsesrådet noterer sig, at indsamlingen af kommunikationsbekræftelsesdata kun kan finde sted på grundlag af en retskendelse. Desuden kræver CPPA, at der gives detaljeret information både i begæringen om retskendelsen og i selve retskendelsen.[64] En sådan forudgående retskendelse har til formål at begrænse retshåndhævende myndigheders skønsmæssige beføjelser ved anvendelse af loven samt kontrollere, om der i de enkelte tilfælde er tilstrækkeligt grundlag for at indsamle kommunikationsbekræftelsesdata. Databeskyttelsesrådet anerkender også, at Republikken Koreas lovgivning ikke synes at indeholde bestemmelser om generel og vilkårlig opbevaring af kommunikationsbekræftelsesdata. Offentlige myndigheders indsigt i disse oplysninger vedrører således altid oplysninger, der fortsat opbevares med henblik på fakturering og levering af selve kommunikationstjenesterne.

[60] Artikel 3, stk. 2 og artikel 2, stk. 6-7, i CPPA.
[61] Artikel 2, stk. 11, i GDPR.
[62] Dette er tilfældet for indholdsdata i henhold til artikel 3, stk. 2, og artikel 5, stk. 1, i CPPA.
[63] Artikel 2 i CPPA's gennemførelsesdekret.
[64] Jf. betragtning 156 i udkastet til afgørelse.

144. EDPD understreger dog, at Domstolen har sat spørgsmålstegn ved, om trafikdata er mindre følsomme end andre data, navnlig indholdsdata.[65] I betragtning af at der gælder et lavere beskyttelsesniveau for kommunikationsbekræftelsesdata end for indholdsdata i flere henseender, opfordrer Databeskyttelsesrådet Europa-Kommissionen til at overvåge omhyggeligt, om de garantier, der er fastsat i Koreas lovgivning for denne kategori af personoplysninger, sikrer et beskyttelsesniveau, der i det væsentlige stemmer overens med niveauet i EU, navnlig med hensyn til lovgivningens proportionalitet og påregnelighed.

4.3. Koreanske offentlige myndigheders indsigt i kommunikationsoplysninger af hensyn til den nationale sikkerhed

145. For så vidt angår de retlige rammer for nationale sikkerhedsmyndigheders indsigt i kommunikationsoplysninger, der overføres fra EØS til Korea, har Databeskyttelsesrådet identificeret to punkter, der giver anledning til bekymring, og som begge vedrører bestemmelserne om indsigt i kommunikation mellem ikke-koreanske statsborgere, der er omfattet af en specifik række anvendelsestilfælde (jf. punkt 29). I disse tilfælde finder bestemte andre garantier ikke anvendelse, for så vidt angår både kommunikationsbekræftelsesdata og indholdsdata. I disse specifikke tilfælde er disse data med andre ord ikke omfattet af de samme garantier som data, der sendes, når mindst én koreansk statsborger er involveret i underretningen.

4.3.1. Ingen forpligtelse til at underrette fysiske personer om offentlige myndigheders indsigt i kommunikation mellem udenlandske statsborgere

146. I et scenarie som beskrevet ovenfor, dvs. hvor ingen af parterne i kommunikationen er koreansk statsborger, er nationale sikkerhedsmyndigheder ikke forpligtet til at underrette fysiske personer om indsamling og behandling af personoplysninger om disse. Databeskyttelsesrådet anerkender, at dette spørgsmål kun berører visse sager. For det første forholder det sig som allerede påpeget sådan, at når mindst én koreansk statsborger er involveret i kommunikationen, gælder underretningskravene i henhold til CPPA for alle parter i kommunikationen uanset deres nationalitet[66] For det andet er indsamlingen af personoplysninger, der stammer fra kommunikation udelukkende mellem udlændinge, omfattet af en specifik række anvendelsestilfælde. I sådanne tilfælde omfatter retten til indsigt navnlig kommunikation fra a) lande, der er fjendtlige over for Republikken Korea, b) udenlandske myndigheder, grupper eller statsborgere, der mistænkes for at deltage i antikoreanske aktiviteter[67], og c) medlemmer af grupper, der har aktiviteter på Den Koreanske Halvø, men reelt uden for Republikken Koreas højhedsområde, og disses paraplygrupper, der er etableret i udlandet. Kommunikation mellem EU-borgere, der overføres fra EØS til Korea, kan således kun indsamles af hensyn til den nationale sikkerhed, hvis den er omfattet af én af de tre ovennævnte kategorier[68]. Som en yderligere begrænsende faktor kunne Databeskyttelsesrådet ud fra Europa-Kommissionens

[65] Jf. Domstolen, C-623/17, *Privacy International*, 6. oktober 2020, ECLI:EU:C:2020:790, præmis 71: "*Indgrebet i den ret, der er fastsat i chartrets artikel 7, og som overførslen af trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne indebærer, skal anses for særligt alvorligt, henset til blandt andet den følsomme karakter af de oplysninger, som disse data kan indeholde, og navnlig muligheden for at udarbejde en profil på de berørte personer på grundlag af disse data, idet sådanne oplysninger ikke er mindre følsomme end selve indholdet af kommunikationen. Desuden kan det hos de berørte personer fremkalde en følelse af, at deres privatliv konstant overvåges (jf., analogt, dom af 8. april 2014, Digital Rights Ireland and Others, C-293/12 og C-594/12, EU:C:2014:238, præmis 27 og 37, og af 21. december 2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 99 og 100).*"

[66] Jf. betragtning 192 i udkastet til afgørelse.

[67] Jf. bilag II, fodnote 244, ifølge hvilken begrebet antikoreanske aktiviteter henviser til aktiviteter, der truer nationens eksistens og sikkerhed, den demokratiske orden og folkets overlevelse og frihed.

[68] Jf. betragtning 187 i udkastet til afgørelse.

supplerende redegørelse forstå, at den gældende retlige ramme ikke giver mulighed for at aflytte data i transit uden for Korea.

147. Derfor kan kritikaliteten af manglen på et underretningskrav anses for at være begrænset, hvad angår konsekvenserne i praksis. Databeskyttelsesrådet understreger dog betydningen af den (efterfølgende) underretning om offentlige myndigheders indsigt, navnlig med hensyn til at sikre effektive retsmidler. Ifølge Domstolen er underretning "*nødvendig for at give de berørte personer mulighed for at udøve deres rettigheder i henhold til artikel 7 og 8 i chartret om anmodning om indsigt i deres personoplysninger, der har været genstand for de pågældende foranstaltninger, og i givet fald at få sidstnævnte berigtiget eller slettet samt i henhold til artikel 47, første afsnit, i chartret at gøre brug af et effektivt retsmiddel for en domstol*"[69]. Offentlige myndigheders indsigt af hensyn til den nationale sikkerhed omfatter ofte hemmelige overvågningsforanstaltninger, hvilket betyder, at de objekter, der er genstand for overvågningen, dvs. de registrerede, ikke er bekendt med behandlingen af deres oplysninger. Således "*har den berørte person i princippet kun få muligheder for retslig prøvelse, medmindre personen underrettes om de foranstaltninger, der er truffet uden vedkommendes viden, og dermed har mulighed for at få prøvet foranstaltningernes lovlighed retsligt med tilbagevirkende kraft, eller, alternativt, medmindre en person, der har mistanke om, at vedkommendes kommunikation bliver eller er blevet aflyttet, kan anlægge sag ved domstolene, således at domstolenes jurisdiktion ikke er afhængig af, at den person, hvis kommunikation er blevet aflyttet, er blevet underrettet*"[70]. I den forbindelse og i overensstemmelse hermed har Databeskyttelsesrådet gentagne gange udtrykt bekymring med hensyn til effektive retsmidler i overvågningssager. Databeskyttelsesrådet understreger, at hemmeligholdelsen af offentlige myndigheders foranstaltninger ikke må føre til, at sådanne foranstaltninger reelt ikke kan anfægtes. På den baggrund skal spørgsmålet om, hvorvidt manglen på et underretningskrav for kommunikation mellem udenlandske statsborgere påvirker databeskyttelsesniveauet som vurderet i udkastet til afgørelse, vurderes som led i en samlet vurdering med særligt hensyn til de tilsyns-, klage- og søgsmålsmekanismer, der er fastsat i den koreanske lovgivning (jf. afsnit 4.7 og 4.8).

148. Desuden bemærker Databeskyttelsesrådet i den forbindelse, at lovgivningen anvender temmelig brede udtryk som antikoreanske eller antinationale aktiviteter,[71] og at det er vanskeligt at forudse, hvordan disse begreber fortolkes i henhold til koreansk ret. Databeskyttelsesrådet opfordrer Europa-Kommissionen til at overvåge, hvordan disse udtryk konkretiseres i koreansk ret, og om deres anvendelse i praksis opfylder de krav om proportionalitet, der følger af EU-retten.

4.3.2. Ingen forudgående uafhængig tilladelse til indsamling af kommunikationsoplysninger mellem udenlandske statsborgere

149. I tilfælde, hvor EØS-personoplysninger, der stammer fra kommunikation mellem ikke-koreanske statsborgere (og som er omfattet af ovennævnte anvendelsestilfælde), skal behandles i Korea af hensyn til den nationale sikkerhed, skal indsamlingen af sådanne oplysninger ikke forhåndsgodkendes af et uafhængigt organ (som det er tilfældet for kommunikation, hvor mindst én af de berørte personer er koreansk statsborger).[72]

---

[69] Domstolen, forenede sager C-511/18, C-512/18 og C-520/18, *La Quadrature du Net and others*, 6. oktober 2020, ECLI:EU:C:2020:791, præmis 190.

[70] Den Europæiske Menneskerettighedsdomstol, *Big Brother Watch and others v. UK*, 25. maj 2021, ECLI:CE:ECHR:2021:0525JUD005817013, præmis 337 og Den Europæiske Menneskerettighedsdomstol, *Case of Roman Zakharov v. Russia*, 4. december 2015, ECLI:CE:ECHR:2015:1204JUD004714306, præmis 234.

[71] Europa-Kommissionen har oplyst, at dette ifølge den koreanske regerings redegørelse henviser til "aktiviteter, der truer nationens eksistens og sikkerhed, den demokratiske orden eller befolkningens overlevelse og frihed", se også fodnote 319 i udkastet til afgørelse om et tilstrækkeligt beskyttelsesniveau.

[72] Jf. betragtning 190 i udkastet til afgørelse.

150. Navnlig i lyset af de seneste afgørelser fra Den Europæiske Menneskerettighedsdomstol ("**ECHR**") "Big Brother Watch and Others v. UK" og "Centrum för Rättvisa v. Sweden" finder Databeskyttelsesrådet det nødvendigt at undersøge, om dette udgør en kritisk mangel ved den koreanske ramme for databeskyttelse. I den forbindelse minder Databeskyttelsesrådet om, som understreget i dets opdaterede anbefalinger om de europæiske væsentlige garantier for overvågningsforanstaltninger,[73] at artikel 6, stk. 3, i traktaten om Den Europæiske Union fastsætter, at de grundlæggende rettigheder, der er forankret i EMRK, udgør generelle principper i EU-retten, mens sidstnævnte, som Domstolen minder om i sin retspraksis, ikke udgør et retligt instrument, der formelt er indarbejdet i EU-retten, så længe Den Europæiske Union ikke har tiltrådt den.[74] Niveauet for beskyttelsen af de grundlæggende rettigheder i henhold til artikel 45 i GDPR skal således fastlægges på baggrund af bestemmelserne i den retsakt, læst i sammenhæng med de grundlæggende rettigheder, der er forankret i chartret. Når det er sagt, har de rettigheder, der er indeholdt i chartret, og som svarer til de rettigheder, der er sikret ved EMRK, i henhold til chartrets artikel 52, stk. 3, samme betydning og rækkevidde som de rettigheder, der er fastsat i den konvention. Der skal derfor tages hensyn til ECHR's retspraksis med hensyn til rettigheder, der også er fastsat i chartret, som en tærskel for minimumsbeskyttelse med henblik på at fortolke tilsvarende rettigheder i chartret, dvs. i det omfang chartret, som fortolket af Domstolen, ikke fastsætter et højere beskyttelsesniveau.[75]

151. Databeskyttelsesrådet bemærker, at selv om forudgående (uafhængig) godkendelse af overvågningsforanstaltninger anses for at være en vigtig garanti mod vilkårlighed, kan en sådan godkendelse ikke udledes af Domstolens retspraksis som et absolut krav om tilsynsforanstaltningernes proportionalitet. ECHR har imidlertid nu udtrykkeligt fastsat kravet om forudgående uafhængig tilladelse til masseaflytning.[76] Selv om det ikke udtrykkeligt fremgår af udkastet til afgørelse, kan Databeskyttelsesrådet forstå, at Republikken Koreas retlige ramme ikke giver mulighed for masseaflytning, men kun for målrettet aflytning af telekommunikation[77]. Europa-Kommissionen har bekræftet denne forståelse.

152. Når det er sagt, viser ovennævnte afgørelser fra ECHR, i overensstemmelse med Domstolens retspraksis [78]og ECHR's tidligere retspraksis[79], endnu en gang betydningen af et omfattende tilsyn fra uafhængige tilsynsmyndigheders side. Databeskyttelsesrådet understreger, at uafhængigt tilsyn i alle faser af processen for offentlige myndigheders indsigt med henblik på retshåndhævelse og af hensyn til den nationale sikkerhed er en vigtig garanti mod vilkårlige overvågningsforanstaltninger og dermed for vurderingen af, om databeskyttelsesniveauet er tilstrækkeligt. Garantien for tilsynsmyndighedernes uafhængighed i den i artikel 8, stk. 3, i chartret anvendte betydning har til formål at sikre effektiv og pålidelig overvågning af, at reglerne om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger overholdes. Det gælder navnlig i tilfælde, hvor den

[73] Jf. Databeskyttelsesrådets anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, punkt 10, 11.
[74] Jf. Domstolen, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems*, 16. juli 2020, ECLI:EU:C:2020:559 (i det følgende benævnt "*Schrems II*"), præmis 98.
[75] Jf. Domstolen, forenede sager C-511/18, C-512/18 og C-520/18, *La Quadrature du Net and others*, 6. oktober 2020, præmis 124.
[76] Jf. ECHR, *Big Brother Watch and others v. UK*, 25. maj 2021, ECLI:CE:ECHR:2021:0525JUD005817013, præmis 351: "Masseaflytning bør fra begyndelsen kun kunne finde sted, hvis der foreligger en uafhængig godkendelse", "masseaflytning bør godkendes af et uafhængigt organ; dvs. et organ, der er uafhængigt af den udøvende magt".
[77] Kun bilag II, afsnit 3.2, indeholder en udtrykkelig erklæring om hensyn til den nationale sikkerhed, når det præciseres, at begrænsningerne og garantierne "*sikrer, at indsamling og behandling af oplysninger begrænses til, hvad der er strengt nødvendigt for at nå et legitimt mål. Det betyder, at masse- og vilkårlig indsamling af personoplysninger af hensyn til den nationale sikkerhed ikke er omfattet*".
[78] Jf. f.eks., Domstolen, forenede sager C-203/15 og C-698/15, *Tele2 Sverige AB and others*, ECLI:EU:C:2016:970.
[79] Jf. f.eks., ECHR, *Case of Roman Zakharov v. Russia*, 4. december 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

pågældende person, på grund af den hemmelige overvågnings karakter, er forhindret i at prøve lovligheden eller at deltage direkte i et søgsmål om lovlighed forud for eller under gennemførelsen af overvågningsforanstaltningen.

153. Manglen på forudgående uafhængig godkendelse kan ikke i sig selv anses som en væsentlig mangel i koreansk ret med hensyn til vurderingen af, om databeskyttelsesniveauet i det væsentlige stemmer overens med niveauet i EU. Vurderingen af tilstrækkeligheden afhænger, igen, af alle sagens omstændigheder, navnlig effektiviteten af efterfølgende tilsyn og adgang til retslig prøvelse som fastsat i Koreas retlige ramme (jf. desuden afsnit 4.7 og 4.8).

4.4. Frivillig videregivelse af personoplysninger

154. I henhold til artikel 83, stk. 3, i TBA kan udbydere af telekommunikationstjenester frivilligt overdrage såkaldte "abonnentdata" [80]til nationale sikkerhedsmyndigheder og retshåndhævende myndigheder efter anmodning. Databeskyttelsesrådet bemærker, at sager vedrørende personoplysninger, der er blevet overført fra EØS til Korea, må forventes at forekomme sjældent, men de skal alligevel analyseres for at vurdere databeskyttelsesniveauet, som allerede nævnt ovenfor.

155. Databeskyttelsesrådet kan forstå, at databeskyttelsesgarantierne i PIPA finder anvendelse i disse tilfælde, at offentlige myndigheder og teletjenesteudbydere skal overholde disse krav[81], og at begge parter kan holdes ansvarlige for enhver krænkelse af de berørte registreredes rettigheder og frihedsrettigheder[82]. Databeskyttelsesrådet kan desuden forstå, at teletjenesteudbydere ikke er forpligtet til at efterkomme sådanne anmodninger.

156. Hvad angår nationale myndigheders indsigt i abonnentdata med henblik på retshåndhævelse samt og navnlig af hensyn til den nationale sikkerhed gennem teleoperatørers "frivillige videregivelse", er Databeskyttelsesrådet imidlertid bekymret for en øget risiko for registreredes rettigheder og frihedsrettigheder, navnlig med hensyn til deres ret til underretning.

157. I henhold til artikel 58, stk. 1, litra 2), i PIPA finder bestemmelserne i kapitel III-VII ikke anvendelse på personoplysninger, som der anmodes om i forbindelse med den nationale sikkerhed. I den henseende finder f.eks. bestemmelserne i artikel 18 (begrænsning af brug uden for formål og afgivelse af personoplysninger) og artikel 20 (underretning om kilder osv. til personoplysninger indsamlet fra tredjemand) i PIPA ikke anvendelse på sådanne anmodninger. I tilfælde, hvor en anmodning fremsættes af en national sikkerhedsmyndighed, rejser dette for det første spørgsmålet om, hvorvidt artikel 58, stk. 1, litra 2), også betyder, at PIPA ikke finder anvendelse på teletjenesteudbydere. På den anden side opstår spørgsmålet, om udelukkelsen af anvendelsen af artikel 20 i PIPA i sådanne tilfælde også gælder for den tilsvarende bestemmelse i afsnit 3 i bilag I (underretning om oplysninger, hvis personoplysninger ikke er indhentet fra den registrerede (lovens artikel 20)). Hvis dette var tilfældet, og hvis artikel 58, stk. 1, litra 2), også var rettet mod teletjenesteudbydere, ville der ifølge den foreliggende information være en risiko for, at der ikke ville være en retlig forpligtelse til at underrette de registrerede om den frivillige videregivelse af personoplysninger.

158. EDPD er derfor bekymret for effektiviteten, dvs. at underretningskravene kan vise sig ineffektive og gøre det betydeligt vanskeligere for registrerede at gøre deres databeskyttelsesmæssige rettigheder gældende, navnlig hvad angår retslig prøvelse. I den forbindelse opfordrer Databeskyttelsesrådet Europa-Kommissionen til at præcisere anvendelsesområdet for de relevante bestemmelser.

---

[80] Relevante datasæt er: brugeres navn, personregistreringsnummer, adresse og telefonnummer, datoer for, hvornår brugere tegner eller opsiger deres abonnement, samt brugeridentifikationskoder (anvendes til at identificere den retmæssige bruger af computersystemer eller kommunikationsnet).

[81] Jf. betragtning 164 og 194 i udkastet til afgørelse.

[82] Jf. betragtning 166 i udkastet til afgørelse.

4.5. Videre anvendelse af oplysninger

159. Princippet om formålsbegrænsning er et centralt lovkrav i forbindelse med databeskyttelse. Det kræver, at personoplysninger kun indsamles til nærmere angivne, eksplicitte og legitime formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål. Desuden har offentlige myndigheder i henhold til EU-retten lov til at behandle personoplysninger med henblik på forebyggelse, efterforskning eller retsforfølgning af strafbare handlinger, selv om oplysningerne oprindeligt blev indhentet til et andet formål, hvis de pågældende myndigheder har et retsgrundlag til at behandle oplysningerne i henhold til den relevante lovgivning, og hvis viderebehandlingen ikke står i misforhold[83].

160. På den baggrund bemærker Databeskyttelsesrådet, at den koreanske ramme for databeskyttelse fastsætter garantier og begrænsninger, der svarer til dem, der er fastsat i EU-retten, hvad angår videre anvendelse af personoplysninger, der er indsamlet med henblik på retshåndhævelse og af hensyn til den nationale sikkerhed, f.eks. artikel 3, stk. 1-2, i PIPA om princippet om formålsbegrænsning.

4.6. Videreoverførsel og udveksling af efterretninger

161. Ifølge artikel 44 i GDPR må videregivelse og videreoverførsel af personoplysninger kun finde sted, hvis det beskyttelsesniveau, som garanteres i medfør af GDPR, ikke undermineres. Beskyttelsesniveauet for personoplysninger, der overføres fra EØS til Korea, må således ikke undermineres af videreoverførslen til modtagere i et tredjeland, dvs. at videreoverførsel kun bør tillades, hvis der er sikkerhed for, at beskyttelsesniveauet fortsat i det væsentlige stemmer overens med det niveau, der er fastsat i EU-retten. Ved vurderingen af, om et tredjeland sikrer et tilstrækkeligt niveau for databeskyttelse, skal der derfor tages hensyn til landets retlige ramme for videreoverførsel. Dette er uomtvisteligt og i overensstemmelse med både Europa-Kommissionens[84] og Databeskyttelsesrådets opfattelse.

162. I den forbindelse noterer Databeskyttelsesrådet sig, at ECHR i sine nylige afgørelser "Big Brother Watch and Others v. UK" og "Centrum för Rättvisa v. Sweden" har givet vejledning[85] om de forholdsregler i forbindelse med databeskyttelse, der skal iagttages i kontraherende stater, når de videregiver personoplysninger til andre parter med henblik på retshåndhævelse og af hensyn til den nationale sikkerhed i sager om masseindsamling. "*For det første skal det klart fremgå af national ret, under hvilke omstændigheder en sådan overførsel kan finde sted. For det andet skal den videregivende stat sikre, at modtagerstaten ved behandlingen af oplysningerne har indført garantier, der kan forhindre misbrug og uforholdsmæssige indgreb. Modtagerstaten skal navnlig garantere sikker opbevaring af materialet og begrænse dets videregivelse. [...] For det tredje vil der være behov for skærpede garantier, når det er klart, at materiale, der kræver særlig fortrolighed — såsom fortroligt journalistisk materiale — overføres.*"[86]

163. Ved anvendelsen af disse standarder fandt ECHR i "*Centrum för Rättvisa v. Sweden*", at fraværet af et udtrykkeligt lovkrav i aflytningssystemet om at vurdere nødvendigheden og proportionaliteten af udveksling af efterretninger for de mulige konsekvenser for retten til privatlivets fred udgør en overtrædelse af artikel 8 i EMRK. ECHR kritiserede, at aflytningsmateriale som følge af lovgivningens

[83] Se artikel 4, stk. 2, i LED.
[84] Jf. betragtning 84 ff. i udkastet til afgørelse.
[85] Følgende elementer blev fastlagt i forbindelse med sagerne *Big Brother Watch* og *Centrum för Rättvisa*, som vedrører masseaflytningssystemer. Kravet om forholdsregler, der skal træffes ved videregivelse af materiale til andre parter, indgik allerede i de kriterier, som ECHR udviklede i forbindelse med målrettet aflytning, og var ikke blevet yderligere præciseret af ECHR (jf. *Big Brother Watch and Others v. UK*, præmis 335 og 362).
[86] ECHR, *Big Brother Watch and Others v. UK*, 25. maj 2021, ECLI:CE:ECHR:2021:0525JUD005817013, præmis 362.

generelle karakter generelt kan sendes til udlandet, når dette anses for at være i national interesse, uanset om den udenlandske modtager har et acceptabelt minimumsniveau med hensyn til garantier[87]

164. I erkendelse af, at de sydkoreanske retlige rammer ikke giver mulighed for masseaflytning, mener Databeskyttelsesrådet, stadig i lyset af konsekvenserne af ECHR's retspraksis som beskrevet ovenfor, at ud over de krav, der følger af EU-retten som fortolket af Domstolen, bør ECHR's argumentation tages i betragtning ved vurderingen af, om den retlige ramme for videreoverførsel til et tredjeland sikrer tilstrækkelige databeskyttelsesstandarder.

1.6.1. Gældende retlige rammer for videreoverførsel fra retshåndhævende myndigheder

165. Med hensyn til videreoverførsel fra de kompetente myndigheder med henblik på retshåndhævelse kan Databeskyttelsesrådet ud fra Europa-Kommissionens redegørelse forstå, at afsnit 2 i bilag I til udkastet til afgørelse om begrænsning af videreoverførsel finder anvendelse, herunder når overførslen finder sted på grundlag af en anden statut end PIPA. Det fremgår af denne regel, at "*hvis personoplysninger videregives til en tredjemand i udlandet, er de som følge af forskelle i de forskellige landes systemer til beskyttelse af personoplysninger ikke nødvendigvis omfattet af det beskyttelsesniveau, der er garanteret i Koreas lov om beskyttelse af personoplysninger. Sådanne tilfælde vil derfor blive betragtet som 'tilfælde, hvor der kan opstå ulemper for den registrerede' som omhandlet i artikel 17, stk. 4, i loven eller 'tilfælde, hvor den registreredes eller tredjemands interesser krænkes illoyalt' som omhandlet i artikel 18, stk. 2, i loven og artikel 14, stk. 2, i gennemførelsesdekretet for samme lov. For at opfylde kravene i disse bestemmelser skal den persondataansvarlige og tredjemanden derfor udtrykkeligt sikre et beskyttelsesniveau svarende til lovens, herunder garanti for den registreredes udøvelse af sine rettigheder i juridisk bindende dokumenter såsom kontrakter, også efter overførsel af personoplysninger til udlandet"*[88].

166. Databeskyttelsesrådet bifalder denne bestemmelse, som, hvis det antages, at databeskyttelsesniveauet i Korea er tilstrækkeligt til dette formål, sikrer kontinuiteten i et beskyttelsesniveau, der i det væsentlige stemmer overens med niveauet for videreoverførsel i EU-retten. Kommissionen har bekræftet, at Databeskyttelsesrådets opfattelse, dvs. at dette afsnit i bilag I finder anvendelse på al videreoverførsel foretaget af de kompetente myndigheder med henblik på retshåndhævelse, er korrekt. Databeskyttelsesrådet påpeger dog, at det skal sikres, at denne retsakt sikrer et fortsat beskyttelsesniveau i praksis, da der kan være usikkerhed om, hvilke kontraktmæssige garantier og forpligtelser eller andre lignende mekanismer der kan anvendes til at opnå et sådant beskyttelsesniveau i tilfælde af behandling med henblik på retshåndhævelse. I den forbindelse bør det yderligere anføres, f.eks. at personoplysninger kun må videregives til de relevante kompetente myndigheder i tredjelandet.

167. Med forbehold af ovenstående præcisering af, hvorvidt KOFIU er omfattet af udkastet til afgørelse, bemærker Databeskyttelsesrådet, at det i den officielle erklæring om offentlige myndigheders indsigt[89] oplyses, at direktøren for KOFIU i henhold til artikel 8, stk. 1, i ARUSFTI kan videregive bestemte oplysninger om finansielle transaktioner til udenlandske finansielle efterretningstjenester, hvis det skønnes nødvendigt for at opfylde ARUSFTI's formål.[90] Artikel 8 i ARUSFTI indeholder ikke i sig selv en forpligtelse til at afgøre, om det pågældende land stiller tilstrækkelige

[87] Jf. ECHR, *Centrum för Rättvisa v. Sweden*, 25. maj 2021, ECLI:CE:ECHR:2021:0525JUD003525208, præmis 326.
[88] Udkast til afgørelse, bilag I, s. 7.
[89] Jf. udkast til afgørelse, bilag II.
[90] Jf. udkast til afgørelse, bilag II, afsnit 2.2.3.2. Selv om en sådan udveksling kun må finde sted på betingelse af, at den udenlandske tjeneste ikke anvender oplysningerne til et andet formål end det oprindelige formål med videregivelsen og navnlig ikke til en strafferetlig efterforskning eller retssag (artikel 8, stk. 2, i ARUSFTI), kan direktøren for KOFIU efter anmodning fra et andet land give samtykke til anvendelse af sådanne oplysninger til strafferetlig efterforskning eller retsforfølgning af strafbare handlinger med justitsministerens forudgående samtykke (artikel 8, stk. 3, i ARUSFTI).

databeskyttelsesgarantier, og i givet fald sikre dette. Bilag II henviser ikke til det nye afsnit i bilag I i denne henseende. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at præcisere sammenhængen mellem det relevante afsnit i bilag I om begrænsning af videreoverførsel og retsgrundlaget for videreoverførsel i henhold til ARUSFTI.

4.6.2. Gældende retlige rammer for videreoverførsel af hensyn til den nationale sikkerhed

168. Udkastet til afgørelse indeholder ingen information om de retlige rammer for videreoverførsel på området national sikkerhed. Derfor kan Databeskyttelsesrådet forstå, at afsnit 2 i bilag I, til forskel fra til retshåndhævelsesformål, ikke finder anvendelse på videreoverførsel af hensyn til den nationale sikkerhed. Artikel 17 og 18 i PIPA, som er omfattet af det pågældende afsnit i bilag I, er en del af kapitel III i PIPA, som til gengæld ikke finder anvendelse på behandling af personoplysninger af hensyn til den nationale sikkerhed (artikel 58, stk. 1, i PIPA).

169. Databeskyttelsesrådet antager imidlertid, at Korea kan have behov for at overføre og overfører personoplysninger til udenlandske efterretningstjenester af hensyn til den nationale sikkerhed, blandt andet for at samarbejde om at bekæmpe grænseoverskridende trusler mod den nationale sikkerhed og for at advare udenlandske regeringer om eller anmode om deres hjælp til at identificere sådanne trusler.

170. Databeskyttelsesrådet kunne forstå, at videreoverførsel efter Europa-Kommissionens opfattelse er tilstrækkeligt reguleret i koreansk ret på grundlag af de garantier, der følger af den overordnede forfatningsmæssige ramme, navnlig principperne om nødvendighed og proportionalitet samt af de centrale principper for databeskyttelse, der er reguleret i PIPA, såsom lovlig og rimelig behandling, formålsbegrænsning, dataminimering, sikkerhed og de generelle forpligtelser til at forhindre misbrug af personoplysninger.

171. Databeskyttelsesrådet anerkender den generelle anvendelse af disse centrale principper (for databeskyttelse), men er bekymret over, at disse garantier er af meget generel karakter og ikke specifikt henviser til eller behandler de specifikke omstændigheder og betingelser for videreoverførsel af personoplysninger, der overføres fra EØS af hensyn til den nationale sikkerhed, i et retsgrundlag. Selv om disse generelle og overordnede principper finder bred anvendelse, sætter Databeskyttelsesrådet spørgsmålstegn ved, om dette kan anses for at opfylde kriterierne for klare og præcise regler og for i tilstrækkelig grad at sikre effektive garantier, der kan håndhæves. Navnlig når offentlige myndigheders indsigt i og behandling af personoplysninger udøves i hemmelighed, og de konklusioner, der kan drages af oplysningerne, er særligt alvorlige, er det vigtigt at have klare og detaljerede regler. Lovgivningen bør angive omfanget af eventuelle skønsmæssige beføjelser, der tillægges de kompetente myndigheder, og måden, hvorpå de udøves, med tilstrækkelig klarhed til at give fysiske personer tilstrækkelig beskyttelse. I *Schrems II*-dommen minder Domstolen om, at et retsgrundlag, der tillader indgreb i grundlæggende rettigheder, for at opfylde kravene i nødvendigheds- og proportionalitetsprincippet selv skal definere rækkevidden af begrænsningen af udøvelsen af den pågældende rettighed, fastsætte klare og præcise regler for den pågældende foranstaltnings rækkevidde og anvendelse samt fastsætte minimumsgarantier.[91] Databeskyttelsesrådet er derfor bekymret for, at det ikke er tilstrækkeligt, at sådanne garantier generelt er forankret i højere rangerende lovgivning uden specifikt at implementere f.eks. begrebet proportionalitet i selve det pågældende retsgrundlag.

172. Denne bekymring støttes af ovennævnte afgørelse fra ECHR, hvori domstolen fastslog, at en generel regel uden en udtrykkelig forpligtelse til at vurdere nødvendighed og proportionalitet eller tage privatlivets fred i betragtning ikke er forenelig med retten til privatlivets fred i henhold til artikel 8 i EMRK. I den forbindelse bemærker Databeskyttelsesrådet, at der i den pågældende retspraksis (samt i Koreas lovgivning) findes overordnede (forfatningsmæssigt garanterede) principper om

[91] Jf. *Schrems II*, præmis 175 og 180.

nødvendighed og proportionalitet, blandt andet i henhold til chartret og gennem tiltrædelsen af EMRK.

173. Databeskyttelsesrådet opfordrer Europa-Kommissionen til at præcisere retsgrundlaget, hvordan og i hvilket omfang og under hvilke specifikke betingelser efterretningstjenester er forpligtet til at tage bekymringer vedrørende privatlivets fred og databeskyttelsesgarantier i betragtning, inden de videregiver personoplysninger til udenlandske partnere af hensyn til den nationale sikkerhed. Hvis en sådan forpligtelse følger direkte af forfatningsmæssige principper, bør Europa-Kommissionen desuden vurdere kravene om præcision og klarhed i den relevante lovgivning og bekræfte, at de generelle forfatningsmæssige principper og databeskyttelsesprincipper anvendes og gennemføres korrekt.

4.6.3. Internationale aftaler

174. Databeskyttelsesrådet bemærker, at Europa-Kommissionen i forbindelse med sin vurdering af beskyttelsesniveauets tilstrækkelighed ikke tog hensyn til eksistensen af internationale aftaler mellem Republikken Korea og tredjelande eller internationale organisationer, der kan fastsætte specifikke bestemmelser for retshåndhævende myndigheders og/eller efterretningstjenesters internationale overførsel af personoplysninger til tredjelande. Databeskyttelsesrådet finder, at indgåelsen af bilaterale eller multilaterale aftaler med tredjelande med henblik på samarbejde på retshåndhævelses- eller efterretningsområdet må forventes at påvirke Koreas retlige ramme for databeskyttelse som vurderet.

175. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at præcisere, om der findes sådanne aftaler, og på hvilke betingelser de kan indgås, samt vurdere, om bestemmelserne i internationale aftaler kan påvirke beskyttelsesniveauet for personoplysninger, der overføres fra EØS til Korea i henhold til den retlige ramme og praksis i forbindelse med international videregivelse med henblik på retshåndhævelse og af hensyn til den nationale sikkerhed.

4.7. Tilsyn

176. Databeskyttelsesrådet bemærker, at tilsynet med retshåndhævende myndigheder på det strafferetlige område og nationale sikkerhedsmyndigheder sikres ved en kombination af en række interne og eksterne organer.

177. I den forbindelse skal det bemærkes, at Domstolen gentagne gange har understreget behovet for et uafhængigt tilsyn som et væsentligt element i beskyttelsen af fysiske personer i forbindelse med behandling af deres personoplysninger. Begrebet uafhængighed omfatter områderne institutionel autonomi, frihed for instrukser samt materiel uafhængighed. For at sikre konsekvent overvågning og håndhævelse af databeskyttelseslovgivningen skal tilsynsmyndigheder have reelle beføjelser, herunder beføjelser til at træffe afhjælpende foranstaltninger.

178. Databeskyttelsesrådet er enigt i Europa-Kommissionens konklusion om, at Korea i en samlet vurdering kan anses for at have et uafhængigt og effektivt tilsynssystem, selv om en række organer i tilsynssystemet ikke i sig selv opfylder ovennævnte krav. F.eks. har de fleste af dem ikke udøvende beføjelser, men er begrænset til at arbejde med rene henstillinger, blandt andet den nationale menneskerettighedskommission og revisions- og inspektionsrådet. Desuden er hovedparten af de pågældende offentlige myndigheder ikke udelukkende databeskyttelsesinstitutioner, men har normalt andre opgaver på området for beskyttelse af grundlæggende rettigheder.

179. På baggrund af Europa-Kommissionens redegørelse bemærker Databeskyttelsesrådet dog, at tilsynet med de retshåndhævende myndigheder er omfattende og uden undtagelse garanteret af PIPC. PIPC har derfor i henhold til PIPA og andre databeskyttelseslove (blandt andet CPPA) efterforsknings-

afhjælpnings- og håndhævelsesmæssige beføjelser, som gælder for hele området for retshåndhævende myndigheders og nationale sikkerhedsmyndigheders indsigt i personoplysninger.

180. I den forbindelse vil Databeskyttelsesrådet gerne endnu en gang understrege nødvendigheden af, at tilsynsmyndigheder udstyres med tilstrækkelige menneskelige, tekniske og finansielle ressourcer for at kunne udføre deres opgaver og varetage deres beføjelser. I den forbindelse mangler der desværre information om de udpegede tilsynsorganer, navnlig PIPC. Databeskyttelsesrådet gentager derfor sin anmodning til Europa-Kommissionen om at fremlægge yderligere information om dette.

181. Generelt vil Databeskyttelsesrådet gerne bemærke, at der stort set ikke er erklæringer, eksempler eller tal i udkastet til afgørelse vedrørende tilsynsaktiviteterne og tilsynsorganernes retshåndhævelse af databeskyttelseslovgivningen på områderne retshåndhævelse og national sikkerhed. Dette ville være nyttigt i forbindelse med evalueringen af tilsynsorganernes effektivitet.

1.8. Retsmidler

182. Databeskyttelsesrådet minder om, at det er afgørende for et tilstrækkeligt databeskyttelsesniveau, at registrerede har adgang til omfattende retsmidler mod uberettiget indsigt i og behandling af oplysninger. Disse retsmidler skal være tilstrækkelige til, at en registreret kan få indsigt i de oplysninger, der opbevares om vedkommende, og at få dem berigtiget eller slettet.

183. I lyset af Domstolens *Schrems I*- og *Schrems II*-domme er det klart, at ud over retten til at henvende sig til kompetente myndigheder er effektiv retlig beskyttelse som omhandlet i artikel 47, stk. 1, i chartret af afgørende betydning for, at det kan antages, at lovgivningen i et tredjeland er tilstrækkelig.

184. Databeskyttelsesrådet anerkender, at Korea har etableret forskellige muligheder for at sikre fysiske personers ret til indsigt, opbevaring, sletning og suspension i henhold til PIPA. Disse rettigheder kan udøves over for den dataansvarlige selv eller via en klage indgivet til PIPC eller andre tilsynsorganer, f.eks. den nationale menneskerettighedskommission. Databeskyttelsesrådet anerkender desuden muligheden for at anfægte dataansvarliges eller offentlige myndigheders afgørelse som svar på en anmodning på grundlag af loven om administrative tvister.

185. Desuden kan Databeskyttelsesrådet ud fra Europa-Kommissionens redegørelse forstå, at fysiske personer kan anfægte de retshåndhævende myndigheders og de nationale sikkerhedsmyndigheders handlinger ved de kompetente domstole i henhold til loven om administrative tvister og loven om forfatningsdomstolen og har mulighed for at opnå erstatning i henhold til loven om statslig erstatning.[92]

186. I den forbindelse er Databeskyttelsesrådet dog bekymret for effektiviteten af administrativ og retslig prøvelse for EU-borgere i sager vedrørende den nationale sikkerhed, hvor der ikke er koreanske statsborgere involveret. Som anført i punkt 33 ff. er de nationale sikkerhedsmyndigheder ikke forpligtet til at underrette registrerede om indsamling og behandling af deres personoplysninger. Da det er betydeligt vanskeligere at opnå effektiv retsbeskyttelse i sådanne sager, vil Databeskyttelsesrådet gerne påpege, at der er behov for bestemte retsgarantier på dette område, hvis der er tale om personoplysninger, der overføres fra EØS. Disse garantier skal sætte registrerede i stand til at gribe effektivt ind over for ulovlig databehandling på en retligt sikker måde uden at blive hindret deri af alt for snævre proceduremæssige krav, f.eks. ved at få pålagt en bevisbyrde, som de ikke kan leve op til uden kendskab til behandlingen. Desuden skal registrerede kunne henvende sig til et kompetent organ, der opfylder kravene i artikel 47 i CFR, dvs. som har kompetence til at fastslå, at en databehandling finder sted, og til at kontrollere lovligheden af behandlingen, samt har beføjelse til at træffe afhjælpende foranstaltninger, hvis databehandlingen er ulovlig. På den baggrund vil en simpel ret til at klage til f.eks. NHRC ikke være tilstrækkelig. Databeskyttelsesrådet opfordrer derfor

[92] Jf. bilag II, 3.2.4 sammenholdt med 2.4.3.

Kommissionen til at redegøre nærmere for, hvordan disse krav gennemføres i proceduremæssig og materiel henseende, f.eks. om det er muligt for registrerede at henvende sig til PIPC samt til en domstol uden at skulle bevise den pågældende databehandling.

187. Desuden bemærker Databeskyttelsesrådet, at udkastet til afgørelse indeholder bestemmelser om en klagemekanisme, dvs. at EU-borgere kan indgive en klage til PIPC gennem deres nationale databeskyttelsesmyndighed eller Databeskyttelsesrådet. PIPC underretter derefter den pågældende via den samme kanal, når undersøgelsen er afsluttet[93]. Databeskyttelsesrådet bifalder bestræbelserne på at gøre adgangen til at klage over koreanske nationale sikkerhedsmyndigheder nemmere. Samtidig slår Databeskyttelsesrådet til lyd for, at en sådan klagemekanisme kanaliseres gennem de europæiske nationale databeskyttelsesmyndigheder frem for Databeskyttelsesrådet, da de er kompetente og tættere på behandlingen af de individuelle klager.

188. Desuden bemærker Databeskyttelsesrådet en mulig modsigelse med hensyn til frivillig afgivelse af personoplysninger. På den ene side fremgår det af udkastet til afgørelse, at fysiske personer kan opnå adgang til administrativ eller retslig prøvelse, hvis deres oplysninger videregives ulovligt efter en anmodning om frivillig videregivelse af personoplysninger, herunder mod den retshåndhævende myndighed, der har fremsat anmodningen.[94] På den anden side henvises der i udkastet til afgørelse til kravet om direkte konsekvenser for den fysiske person ret til at anfægte offentlige myndigheders handlinger, idet (kun) bindende anmodninger om videregivelse nævnes som et eksempel på en sag, hvor en administrativ handling anses for at have direkte konsekvenser for retten til privatlivets fred.[95] Databeskyttelsesrådet kan ud fra Europa-Kommissionens redegørelse forstå, at der rent faktisk ikke er nogen begrænsning i mulighederne for klage eller søgsmål i forbindelse med anmodninger om frivillig videregivelse af personoplysninger, og anmoder derfor Europa-Kommissionen om at præcisere dette nærmere i afgørelsen, både på områderne retshåndhævelse og national sikkerhed (i modsætning til afsnittet om retshåndhævelse indeholder afsnittet om frivillig videregivelse af personoplysninger af hensyn til den nationale sikkerhed ikke en udtrykkelig erklæring om klage- og søgsmålsmuligheder i denne forbindelse).

[93] Jf. betragtning 205 og bilag I, s. 19 i udkastet til afgørelse.
[94] Jf. betragtning 166 i udkastet til afgørelse.
[95] Jf. betragtning 181 (retshåndhævelse) og betragtning 208 og 181 (national sikkerhed) i udkastet til afgørelse.