Henstillinger

Henstilling 01/2021 om henvisning til tilstrækkelighed i henhold til direktivet om retshåndhævelse

Vedtaget den 2. februar 2021

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

Versionshistorik

Udgave 1.1	6. juli 2021	Formateringsændring
Udgave 1.0	2. februar 2021	Vedtagelse af henstillinger

Indholdsfortegnelse

1. INDLEDNING 4

2. BEGREBET ET TILSTRÆKKELIGT BESKYTTELSESNIVEAU 5

3. PROCEDUREMÆSSIGE ASPEKTER I FORBINDELSE MED VURDERING AF ET TILSTRÆKKELIGT BESKYTTELSESNIVEAU I HENHOLD TIL DIREKTIVET OM RETSHÅNDHÆVELSE. 6

4. EU-STANDARDER FOR TILSTRÆKKELIGHEDEN AF POLITISAMARBEJDET OG DET RETLIGE SAMARBEJDE I STRAFFESAGER 8

A. Almindelige principper og garantier 10

a) Begreber 10

b) Lovlig og rimelig behandling af personoplysninger 11

c) Princippet om formålsbegrænsning 11

d) Særlige betingelser for viderebehandling til andre formål 12

e) Dataminimeringsprincippet 12

f) Princippet om oplysningernes rigtighed 13

g) Datalagringsprincippet 13

h) Princippet om sikkerhed og fortrolighed 13

i) Gennemsigtighedsprincippet (artikel 13, betragtning 26, 39, 42, 43, 44 og 46) 13

j) Retten til indsigt, berigtigelse og sletning (artikel 14 og 16) 14

k) Begrænsninger i registreredes rettigheder 14

l) Begrænsning af videreoverførsel (artikel 35, betragtning 64-65) 15

m) Ansvarlighedsprincippet 15

B. Eksempler på yderligere principper, der skal anvendes på specifikke former for behandling 16

a) Særlige kategorier af oplysninger 16

b) Automatiseret beslutningstagning og profilering 16

c) Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger 16

C. Procedure- og håndhævelsesmekanismer 17

a) Kompetent uafhængig tilsynsmyndighed 17

b) Effektiv gennemførelse af databeskyttelsesreglerne 17

c) Databeskyttelsessystemet skal lette udøvelsen af registreredes rettigheder 17

d) Databeskyttelsessystemet skal indeholde passende søgsmålsmekanismer 18

Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet") har —

under henvisning til artikel 51, stk. 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA[1],

under henvisning til artikel 12 og 22 i Databeskyttelsesrådets forretningsorden —

VEDTAGET DISSE HENSTILLINGER

1. INDLEDNING

1. Artikel 29-Gruppen har offentliggjort et arbejdsdokument[2] om henvisning til tilstrækkelighed i henhold til den generelle forordning om databeskyttelse (GDPR)[3]. Dette arbejdsdokument blev godkendt af Det Europæiske Databeskyttelsesråd på dets første plenarmøde.

2. Som anført i erklæring nr. 21, der er knyttet som bilag til Lissabontraktaten, kan specifikke regler om beskyttelse af personoplysninger og fri udveksling af sådanne oplysninger inden for retligt samarbejde i straffesager og politisamarbejde baseret på artikel 16 i traktaten om Den Europæiske Unions funktionsmåde (TEUF) vise sig at være nødvendige på grund af disse områders særlige karakter.

3. På dette grundlag vedtog EU-lovgiveren direktiv (EU) 2016/680 (direktivet om retshåndhævelse), der fastsætter specifikke regler for de kompetente myndigheders behandling af personoplysninger med henblik på at **forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod forebyggelse af trusler mod den offentlige sikkerhed**.

4. Direktivet om retshåndhævelse fastsætter de grunde, der gør det muligt at overføre personoplysninger til et tredjeland eller en international organisation i denne forbindelse. En af betingelserne for en sådan overførsel er Europa-Kommissionens afgørelse om, at det pågældende tredjeland eller den pågældende internationale organisation sikrer et tilstrækkeligt beskyttelsesniveau.

5. Hvor arbejdsdokumentet WP254.rev01 om en reference vedrørende tilstrækkelighed har til formål at vejlede Europa-Kommissionen om databeskyttelsesniveauet i tredjelande og

[1] EUT L 119 af 4.5.2016, s. 89.
[2] WP254.rev01 vedtaget af Artikel 29-Gruppen den 28. november 2017 som senest revideret og vedtaget den 6. februar 2018. Det ajourfører kapitel I i arbejdsdokumentet "Overførsel af personoplysninger til tredjelande: Anvendelse af artikel 25 og 26 i EU's databeskyttelsesdirektiv", WP12, vedtaget af Artikel 29-Gruppen den 24. juli 1998.
[3] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 26. 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 (den generelle forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

internationale organisationer i henhold til GDPR, har dette dokument til formål at give lignende vejledning i henhold til direktivet om retshåndhævelse. Det fastlægger i denne forbindelse de centrale databeskyttelsesprincipper, der skal være til stede i et tredjeland eller en international organisation for at sikre væsentlig ækvivalens med EU databeskyttelsesprincipper inden for rammerne af direktivet om retshåndhævelse (dvs. for kompetente myndigheders behandling af personoplysninger med henblik på forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner). Derudover kan det fungere som en vejledning for tredjelande og internationale organisationer, som er interesserede i at opnå et tilstrækkeligt beskyttelsesniveau.

6. Dette dokument fokuserer udelukkende på afgørelser om tilstrækkeligheden af beskyttelsesniveauet. Der er tale om Europa-Kommissionens gennemførelsesretsakter i henhold til artikel 36, stk. 3, i direktivet om retshåndhævelse.

2. BEGREBET ET TILSTRÆKKELIGT BESKYTTELSESNIVEAU

7. Direktivet om retshåndhævelse fastsætter regler for overførsel af personoplysninger til tredjelande og internationale organisationer, i det omfang sådanne overførsler falder ind under dets anvendelsesområde. Reglerne om international overførsel af personoplysninger er fastsat i kapitel V i direktivet om retshåndhævelse, særlig artikel 35-39.

8. I henhold til artikel 36 i direktivet om retshåndhævelse kan overførsel af oplysninger til et tredjeland eller en international organisation finde sted, hvis et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland eller en international organisation sikrer et tilstrækkeligt beskyttelsesniveau. Det følger af EU-Domstolens retspraksis[4], at denne bestemmelse skal læses i lyset af artikel 35 i direktivet om retshåndhævelse med overskriften "Generelle principper for overførsler af personoplysninger", som fastsætter, at "alle bestemmelserne [i kapitel V i direktivet om retshåndhævelse] anvendes for at sikre, at det beskyttelsesniveau for fysiske personer, som sikres i [direktivet om retshåndhævelse], ikke undermineres".

9. Hvis Europa-Kommissionen har besluttet, at et sådant beskyttelsesniveau er tilstrækkeligt, kan overførsel af personoplysninger til den eller det pågældende tredjeland, territorium, sektor eller internationale organisation finde sted uden at skulle indhente en særlig tilladelse, medmindre en anden medlemsstat, hvorfra oplysningerne er indhentet, skal give tilladelse til overførslen, jf. artikel 35 og 36 og betragtning 66 i direktivet om retshåndhævelse. Dette berører ikke behovet hos myndigheder i de pågældende medlemsstater for at behandle oplysninger med henblik på at overholde de nationale bestemmelser, der er vedtaget i henhold til direktiv (EU) 2016/680.

10. Begrebet "tilstrækkeligt beskyttelsesniveau", som allerede eksisterede i henhold til direktiv 95/46[5] og Rådets rammeafgørelse 2008/977/RIA[6], er blevet videreudviklet af EU-Domstolen i denne forbindelse og for nylig inden for rammerne af GDPR.

[4] Sag C-311/18, Data Protection Commissioner mod Facebook Ireland Ltd og Maximillian Schrems, 16. juli 2020, ECLI:EU:C:2020:559, præmis 92 (Schrems II).
[5] Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281 af 23.11.1995, s. 31).
[6] Rådets rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger behandlet inden for rammerne af politisamarbejde og retligt samarbejde i straffesager (EUT L 350 af 30.12.2008, s. 60).

11. Selv om beskyttelsesniveauet i tredjelandet som anført af EU-Domstolen i det væsentlige skal svare til det, der er sikret i Unionen, kan "de midler, som tredjelandet anvender i denne henseende for at sikre et sådant beskyttelsesniveau, være forskellige fra de midler, som gennemføres inden for Unionen", men "disse midler skal ikke desto mindre vise sig at være effektive"[7]. Standarden for tilstrækkelighed kræver derfor ikke, at EU-lovgivningen afspejles punkt for punkt, men at der fastsættes væsentlige, centrale krav i denne lovgivning.

12. I denne forbindelse præciserede EU-Domstolen også, at en afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet bør indeholde eventuelle konstateringer om, hvorvidt der i tredjelandet findes regler, som er vedtaget af dette land, der tilsigter at begrænse eventuelle indgreb i de grundlæggende rettigheder hos de personer, hvis oplysninger bliver videregivet fra Den Europæiske Union til dette tredjeland, indgreb, som de statslige enheder i dette land er *beføjet* til at foretage, når der herved forfølges legitime mål, såsom statens sikkerhed[8].

13. Formålet med Kommissionens afgørelser om beskyttelsesniveauets tilstrækkelighed er formelt og med bindende virkning for medlemsstaterne[9], herunder deres kompetente databeskyttelsesmyndigheder[10], at fastslå, at databeskyttelsesniveauet i et tredjeland eller en international organisation i det væsentlige svarer til det databeskyttelsesniveau, der er sikret inden for EU. Tredjelandet bør give garantier, der sikrer et passende beskyttelsesniveau, som i det væsentlige svarer til det, der sikres i Unionen, især når oplysninger behandles i en eller flere specifikke sektorer[11].

14. Beskyttelsesniveauets tilstrækkelighed kan opnås ved en kombination af rettigheder for de registrerede og forpligtelser for dem, der behandler data, eller som fører kontrol med en sådan behandling, og uafhængige organers tilsyn. Databeskyttelsesreglerne er imidlertid kun effektive, hvis de kan håndhæves og bliver fulgt i praksis. Der skal derfor ikke kun tages hensyn til indholdet i de regler, der gælder for personoplysninger, som overføres til et tredjeland eller en international organisation, men også til det system, der skal sikre reglernes effektivitet. Effektive håndhævelsesmekanismer er af afgørende betydning for databeskyttelsesreglernes effektivitet[12].

3. PROCEDUREMÆSSIGE ASPEKTER I FORBINDELSE MED VURDERING AF ET TILSTRÆKKELIGT BESKYTTELSESNIVEAU I HENHOLD TIL DIREKTIVET OM RETSHÅNDHÆVELSE.

[7] Sag C−362/14, Maximillian Schrems mod Data Protection Commissioner, 6. oktober 2015, ECLI:EU:C:2015:650, præmis 73 og 74 (Schrems I).
[8] Schrems I, præmis 88.
[9] Artikel 288 i TEUF.
[10] Schrems I, præmis 52.
[11] Betragtning 67 i direktivet om retshåndhævelse.
[12] Schrems I, præmis 72-74, og EU-Domstolens udtalelse 1/15 om udkastet til aftale mellem Canada og Den Europæiske Union, 26. juli 2017, ECLI:EU:C:2017:592 (udtalelse 1/15), præmis 134: "Denne ret til beskyttelse af personoplysninger kræver bl.a., at det ved EU-retten tillagte høje niveau for beskyttelse af de grundlæggende friheder og rettigheder fortsat sikres i tilfælde af overførsel af personoplysninger fra EU til et tredjeland. Selv om de midler, med hvilke det tilsigtes at sikre et sådant beskyttelsesniveau, kan være forskellige fra de midler, som gennemføres inden for Unionen med henblik på at sikre overholdelsen af de krav, der følger af EU-retten, skal disse midler imidlertid i praksis vise sig at være effektive med henblik på at sikre en beskyttelse, der i det væsentlige svarer til den inden for Unionen sikrede beskyttelse."

15. For at kunne opfylde sin opgave med at rådgive Europa-Kommissionen i henhold til artikel 51, stk. 1, litra g), i direktivet om databeskyttelse, skal Databeskyttelsesrådet modtage al relevant dokumentation, herunder relevant korrespondance og Kommissionens konklusioner. Det er absolut nødvendigt, at alle relevante dokumenter fremsendes i tilstrækkelig god tid og oversættes til engelsk til Databeskyttelsesrådet for at muliggøre informerede og nyttige drøftelser inden den endelige vedtagelse af afgørelser om tilstrækkeligheden af beskyttelsesniveauet. Når den retlige ramme er kompleks, bør dette omfatte alle rapporter udarbejdet om databeskyttelsesniveauet i tredjelandet eller den internationale organisation. Under alle omstændigheder bør oplysningerne fra Europa-Kommissionen være udtømmende og sætte Databeskyttelsesrådet i stand til at vurdere den analyse, som Kommissionen har foretaget vedrørende databeskyttelsesniveauet i tredjelandet eller den internationale organisation.

16. Databeskyttelsesrådet vil rettidigt afgive en udtalelse om Kommissionens resultater, identificere eventuelle mangler i tilstrækkelighedsrammen og fremsætte eventuelle anbefalinger, hvor det er nødvendigt.

17. Ifølge artikel 36, stk. 4, i direktivet om retshåndhævelse påhviler det Kommissionen løbende at overvåge udviklinger, der kan påvirke virkningen af afgørelser om beskyttelsesniveauets tilstrækkelighed.

18. I artikel 36, stk. 3, i direktivet om retshåndhævelse fastsættes det, at der skal foretages en regelmæssig revision mindst hvert fjerde år. Dette er imidlertid en generel tidsramme, som skal tilpasses de enkelte tredjelande eller internationale organisationer, der er omfattet af en afgørelse om beskyttelsesniveauets tilstrækkelighed. Alt efter forholdene kan det bestemmes at indføre en kortere revisionscyklus. Derudover kan hændelser eller andre oplysninger om eller ændringer af den retlige ramme i tredjelandet eller den pågældende internationale organisation gøre det nødvendigt at foretage en revision før tid. Det synes endvidere passende at foretage en første revision af en helt ny afgørelse om beskyttelsesniveauets tilstrækkelighed ret tidligt og så gradvist tilpasse revisionscyklussen alt efter de opnåede resultater.

19. I lyset af Databeskyttelsesrådets opgave med at afgive udtalelse til Kommissionen skal Databeskyttelsesrådet, hvis et tredjeland, et område eller en eller flere specifikke sektorer i det pågældende tredjeland eller en international organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau, rettidigt modtage relevante oplysninger fra Kommissionen om overvågningen af den relevante udvikling i tredjelandet eller den internationale organisation. Databeskyttelsesrådet bør således holdes orienteret om enhver revisionsproces og revisionsmission i tredjelandet eller den internationale organisation. Databeskyttelsesrådet henstiller til, at det opfordres til at deltage i disse revisionsprocesser og -missioner, som fastsat i afgørelsen om værnet om privatlivets fred og omhandlet i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet vedrørende Japan.

20. Det skal også bemærkes, at Europa-Kommissionen i henhold til artikel 36, stk. 5, i direktivet om retshåndhævelse har beføjelse til, hvis tredjelandet eller den internationale organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau, at ophæve, ændre eller suspendere eksisterende afgørelser om tilstrækkeligheden af beskyttelsesniveauet. Proceduren for ophævelse, ændring eller suspension involverer Databeskyttelsesrådet, idet det anmodes om en udtalelse i overensstemmelse med artikel 51, stk. 1, litra g), i direktivet om retshåndhævelse.

21. Uden at dette berører de retsforfølgende myndigheders beføjelser, bør tilsynsmyndigheder også have beføjelse til at indbringe overtrædelser af dette direktiv for de judicielle myndigheder eller

deltage i retssager[13]. Det følger navnlig af Domstolens dom i Schrems I-sagen, at databeskyttelsesmyndighederne skal kunne anlægge sag ved de nationale domstole, hvis de finder en persons indsigelse mod en afgørelse om beskyttelsesniveauets tilstrækkelighed begrundet[14]. Schrems II-dommen bekræftede denne vurdering[15].

4. EU-STANDARDER FOR TILSTRÆKKELIGHEDEN AF POLITISAMARBEJDET OG DET RETLIGE SAMARBEJDE I STRAFFESAGER

22. Med hensyn til substansen bør afgørelser om tilstrækkeligheden af beskyttelsesniveauet fokusere på vurderingen af den eksisterende lovgivning i det pågældende tredjeland som helhed, i teorien og i praksis, i lyset af de vurderingskriterier, der er fastsat i artikel 36 i direktivet om retshåndhævelse. Et tredjelands eller en international organisations system skal omfatte følgende grundlæggende principper og mekanismer for procedurer og håndhævelse i forbindelse med databeskyttelse.

23. I artikel 36, stk. 2, i direktivet om retshåndhævelse fastsættes de elementer, som Kommissionen skal tage i betragtning ved vurdering af beskyttelsesniveauets tilstrækkelighed i et tredjeland eller en international organisation.

24. Kommissionen tager navnlig hensyn til retsstatsprincippet, respekten for menneskerettighederne og de grundlæggende frihedsrettigheder[16], relevant lovgivning samt gennemførelsen af en sådan lovgivning, effektive rettigheder for registrerede, der kan håndhæves, og effektiv administrativ og retslig klageadgang for de registrerede, hvis personoplysninger videregives, eksistensen og den effektive funktion af en eller flere uafhængige tilsynsmyndigheder samt de internationale forpligtelser, som tredjelandet eller den internationale organisation har indgået.

25. Det er således klart, at enhver fornuftig analyse af beskyttelsesniveauets tilstrækkelighed skal omfatte to grundlæggende elementer: indholdet af de gældende regler og midlerne til at sikre, at

[13] Se artikel 47, stk. 5, og betragtning 82 i direktivet om retshåndhævelse.

[14] Se Schrems I, præmis 65: "I denne henseende påhviler det den nationale lovgiver at fastsætte retsmidler, der gør det muligt for den pågældende nationale tilsynsmyndighed at gøre de klagepunkter, som den finder begrundede, gældende for de nationale domstole, således at disse, såfremt de deler myndighedens tvivl vedrørende gyldigheden af Kommissionens afgørelse, kan foretage en præjudiciel forelæggelse med henblik på en efterprøvelse af denne afgørelses gyldighed".

[15] Se Schrems II, præmis 120: "Selv når der foreligger en afgørelse om tilstrækkeligheden af beskyttelsesniveauet vedtaget af Kommissionen, skal den kompetente nationale tilsynsmyndighed, for hvilken en person har indgivet en klage vedrørende beskyttelse af sine rettigheder og frihedsrettigheder i forbindelse med en behandling af personoplysninger vedrørende den pågældende, således i fuld uafhængighed kunne undersøge, om overførslen af disse oplysninger opfylder de ved databeskyttelsesforordningen fastsatte krav og, hvor det er relevant, kunne anlægge sag ved de nationale domstole, således at disse, såfremt de deler myndighedens tvivl vedrørende gyldigheden af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, kan foretage en præjudiciel forelæggelse med henblik på en efterprøvelse af dennes gyldighed".

[16] Ved vurderingen af tredjelandets retlige ramme bør der tages hensyn til muligheden for at idømme dødsstraf eller enhver form for grusom og umenneskelig behandling på grundlag af oplysninger, der overføres fra EU. Hvis en sådan straf eller behandling er fastsat i tredjelandets lovgivning, bør der findes yderligere garantier i tredjelandets retlige ramme til at sikre, at oplysninger, der overføres fra EU, ikke anvendes til at anmode om, idømme eller fuldbyrde dødsstraf eller nogen form for grusom og umenneskelig behandling (f.eks. en international aftale, der fastsætter betingelser for overførslen, et tilsagn fra tredjelandet om ikke at idømme dødsstraf eller nogen form for grusom og umenneskelig behandling på grundlag af oplysninger overført fra EU eller et moratorium for dødsstraf).

de gennemføres effektivt i praksis. Det påhviler Kommissionen regelmæssigt at kontrollere, at de indførte regler er effektive i praksis.

26. Kernen i de generelle databeskyttelsesprincipper og procedure- og håndhævelseskravene, der kan betragtes som et minimumskrav for, at beskyttelsen er tilstrækkelig, er afledt af EU's charter om grundlæggende rettigheder (chartret) og direktivet om retshåndhævelse. Generelle bestemmelser om databeskyttelse og beskyttelse af privatlivets fred i tredjelandet er ikke tilstrækkelige. Tværtimod skal der indgå specifikke bestemmelser, der konkret omhandler retten til databeskyttelse på retshåndhævelsesområdet, i tredjelandets eller den internationale organisations retlige ramme. Tredjelandet bør give garantier, der sikrer et passende beskyttelsesniveau, som i det væsentlige svarer til det, der sikres i Unionen, og bestemmelserne skal kunne håndhæves.

27. Hvad angår proportionalitetsprincippet[17] fastslog EU-Domstolen endvidere, for så vidt angår medlemsstaternes lovgivning, at spørgsmålet om, hvorvidt en begrænsning af retten til privatlivets fred og retten til databeskyttelse kan være begrundet, på den ene side skal vurderes ved at måle **alvoren af det indgreb**, der følger af en sådan begrænsning[18], og ved at efterprøve, om **betydningen af det mål af almen interesse**, der forfølges med begrænsningen, står i et rimeligt forhold til denne alvor[19].

28. Ifølge EU-Domstolens praksis skal et retsgrundlag, som tillader indgreb i de grundlæggende rettigheder, for at være i overensstemmelse med proportionalitetsprincippet selv definere rækkevidden af begrænsningen af udøvelsen af den pågældende rettighed[20]. Undtagelser fra og begrænsninger af beskyttelsen af personoplysninger skal holdes inden for det strengt nødvendige[21]. For at opfylde dette krav skal den pågældende lovgivning ud over at fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af den pågældende foranstaltning, opstille en række mindstekrav, således at de personer, hvis data er blevet overført, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personoplysninger mod risikoen for misbrug. Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der kan vedtages en foranstaltning om behandling af sådanne oplysninger, hvorved det sikres, at indgrebet begrænses til det strengt nødvendige. Nødvendigheden af at råde over sådanne garantier er så meget desto større, når personoplysningerne er undergivet en automatiseret behandling"[22].

29. Databeskyttelsesrådet har vedtaget henstillinger, der identificerer væsentlige garantier, som afspejler EU-Domstolens og Den Europæiske Menneskerettighedsdomstols retspraksis på området for overvågning, der skal findes i tredjelandets lovgivning i forbindelse med vurdering af indgrebene af sådanne tredjelandes overvågningsforanstaltninger i de registreredes rettigheder, hvis oplysningerne overføres til det pågældende tredjeland i henhold til GDPR[23]. For at vurdere, om betingelserne i artikel 36, stk. 2, litra a), i direktivet om retshåndhævelse er opfyldt, mener

[17] Chartres artikel 52, stk. 1.
[18] Domstolen bemærkede f.eks., at "det indgreb, som indsamlingen af data i realtid, der gør det muligt at lokalisere et terminaludstyr, indebærer, forekommer særlig alvorligt, idet disse data giver de kompetente nationale myndigheder et middel til at foretage præcis og varig sporing af mobiltelefonbrugernes færden (...)" (forenede sager C-511/18, C-512/18 og C-520/18, La Quadrature du Net m.fl., 6. oktober 2020, ECLI:EU:C:2020:791, præmis 187, herunder citeret retspraksis).
[19] La Quadrature du Net m.fl., præmis 131.
[20] Schrems II, præmis 180.
[21] Schrems II, præmis 176, herunder citeret retspraksis.
[22] Schrems II, præmis 176, herunder citeret retspraksis.
[23] Databeskyttelsesrådets henstilling 02/2020 om europæiske væsentlige garantier for overvågningsforanstaltninger, vedtaget den 10. november 2020.

Databeskyttelsesrådet, at de garantier, der er fastsat i disse henstillinger, skal tages i betragtning ved vurderingen af tilstrækkeligheden af et tredjeland i henhold til direktivet om retshåndhævelse på området for overvågning under hensyntagen til yderligere specifikke betingelser på området for overvågning i denne forbindelse.

30. I forbindelse med kravet i artikel 36, stk. 2, litra b), bør tredjelandet ikke blot sikre et effektivt uafhængigt databeskyttelsestilsyn, men også etablere samarbejdsmekanismer med medlemsstaternes databeskyttelsesmyndigheder[24].

31. I forbindelse med kravet i artikel 36, stk. 2, litra c), bør der ud over de internationale forpligtelser, som tredjelandet eller den internationale organisation har indgået, også tages hensyn til de forpligtelser, der følger af tredjelandets eller den internationale organisations deltagelse i multilaterale eller regionale systemer, navnlig med hensyn til beskyttelse af personoplysninger, samt gennemførelsen af sådanne forpligtelser, navnlig tredjelandets tiltrædelse af andre internationale aftaler om databeskyttelse, f.eks. bør Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske med hensyn til automatisk databehandling og tillægsprotokollen hertil blive taget i betragtning (konvention 108[25] og den moderniserede version, konvention 108+). Tredjelandets overholdelse af de principper, der er nedfældet i internationale dokumenter såsom Europarådets praktiske vejledning om anvendelse af personoplysninger i politisektoren: Der kan også tages hensyn til, hvordan personoplysninger beskyttes i forbindelse med bekæmpelse af kriminalitet.

32. En afgørelse om tilstrækkeligheden af beskyttelsesniveauet bør sikre, at det udenlandske system som helhed gennem indholdet af retten til privatlivets fred og retten til databeskyttelse og deres effektive gennemførelse, tilsyn og håndhævelse sikrer det krævede beskyttelsesniveau, herunder for data i transit til dette tredjeland. Som understreget af EU-Domstolen i Schrems II-dommen bør det høje beskyttelsesniveau også sikres, mens data overføres til et tredjeland[26].

33. Endelig bør Kommissionen, når den vedtager en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i et område eller en specifik sektor i et tredjeland, tage hensyn til klare og objektive kriterier, såsom henvisning til specifikke behandlingsaktiviteter eller anvendelsesområdet for gældende retsstandarder og lovgivning i tredjelandet[27].

A. Almindelige principper og garantier

a) Begreber

34. Der bør være indført grundlæggende databeskyttelsesbegreber. Terminologien skal ikke nødvendigvis være den samme som i direktivet om retshåndhævelse, men begreberne bør afspejle og være i overensstemmelse med begreberne i europæisk databeskyttelseslovgivning. Direktivet om retshåndhævelse omfatter eksempelvis følgende vigtige begreber: "personoplysninger", "behandling af personoplysninger", "kompetente myndigheder", "dataansvarlig", "databehandler", "modtager", "følsomme oplysninger", "rigtighed", "profilering", "databeskyttelse gennem design og databeskyttelse gennem standardindstillinger", "tilsynsmyndighed" og "pseudonymisering".

[24] Betragtning 67 i direktivet om retshåndhævelse.
[25] Betragtning 68 i direktivet om retshåndhævelse.
[26] Se præmis 93.
[27] Betragtning 67 i direktivet om retshåndhævelse.

b) Lovlig og rimelig behandling af personoplysninger (artikel 4 — betragtning 26)

35. I henhold til chartrets artikel 8, stk. 2, skal personoplysninger bl.a. behandles "til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag"[28]. I forbindelse med retshåndhævelse bør det dog bemærkes, at udførelsen af de opgaver, der består i at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger, som i henhold til loven institutionelt er overdraget til de kompetente myndigheder, gør det muligt for disse myndigheder at kræve, at fysiske personer efterlever de anmodninger, der fremsættes. I så fald bør den registreredes samtykke ikke udgøre et retsgrundlag for de kompetente myndigheders behandling af personoplysninger[29].

36. Dette retsgrundlag bør fastsætte klare og præcise regler for omfanget og anvendelsen af de relevante databehandlingsaktiviteter og indførelsen af minimumsgarantier[30]. Desuden mindede EU-Domstolen om, at "lovgivning skal være retligt bindende i national ret"[31].

37. For at være lovlig bør databehandlingen[32] være nødvendig for udførelsen af en opgave, der udføres af en kompetent myndighed med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder garantier mod og forebyggelse af trusler mod den offentlige sikkerhed[33]. Disse formål bør fastsættes i national ret.

38. Personoplysninger skal behandles rimeligt. Databeskyttelsesprincippet om rimelig behandling er et særskilt begreb i forhold til retten til en retfærdig rettergang som defineret i chartrets artikel 47 og artikel 6 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (EMRK)[34].

c) Princippet om formålsbegrænsning (artikel 4)

39. De specifikke formål med behandlingen af personoplysninger bør være udtrykkelige og legitime og fastlagt, når personoplysningerne indsamles[35].

40. Oplysninger bør behandles til et specifikt, udtrykkeligt og legitimt formål med henblik på forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller

[28] Se Schrems II, præmis 173.

[29] Det fremgår også af betragtning 35 i direktivet om retshåndhævelse, at "Hvis det kræves, at den registrerede opfylder en retlig forpligtelse, har den registrerede ikke et reelt og frit valg, hvorfor den registreredes reaktion ikke kan anses for at være en frivillig viljetilkendegivelse. Dette bør ikke forhindre medlemsstaterne i ved lov at fastsætte bestemmelser om, at den registrerede kan acceptere behandling af vedkommendes personoplysninger med henblik på dette direktiv, som f.eks. DNA-test i strafferetlige efterforskninger eller elektronisk overvågning af vedkommendes geografiske position ved elektronisk fodlænke med henblik på fuldbyrdelse af strafferetlige sanktioner".

[30] Se Schrems II, præmis 175 og præmis 180, og udtalelse 1/15, præmis 139, og den deri nævnte retspraksis.

[31] Se sag C-623/17, Privacy International mod Secretary of State for Foreign and Commonwealth Affairs m.fl., 6. oktober 2020, ECLI:EU:C:2020:790, præmis 68 — Det bør også være klart, at EU-Domstolen i den franske version af dommen anvender ordet "*réglementation*", som dækker bredere end kun Parlamentets retsakter.

[32] Behandling af personoplysninger, der helt eller delvis foretages automatisk, og anden behandling end automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

[33] Kompetente myndigheder er enhver offentlig myndighed, der er kompetent hertil, eller ethvert andet organ eller enhver anden enhed, der ved lov er bemyndiget til at udøve offentlig myndighed og offentlige beføjelser med henblik herpå.

[34] Betragtning 26 i direktivet om retshåndhævelse.

[35] Betragtning 26 i direktivet om retshåndhævelse.

fuldbyrdelse af strafferetlige sanktioner[36], herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed i tredjelandet, og bør følgelig anvendes til disse formål, for så vidt dette ikke er uforeneligt med det oprindelige formål med behandlingen (f.eks. med henblik på parallelle håndhævelsesprocedurer eller arkivering i samfundets interesse, videnskabelig, statistisk eller historisk anvendelse til sådanne formål) og med forbehold af passende garantier for registreredes rettigheder og frihedsrettigheder. Hvis personoplysninger behandles af den samme eller en anden dataansvarlig (kompetent myndighed[37]) med henblik på at forebygge, efterforske, opdage eller retsforfølge strafbare handlinger eller fuldbyrde andre strafferetlige sanktioner end dem, hvortil de er indsamlet, bør en sådan behandling være tilladt på den betingelse, at en sådan behandling er tilladt i overensstemmelse med gældende retlige bestemmelser og er nødvendig til og står i rimeligt forhold til dette andet formål[38]. Der bør også tages hensyn til, at der findes en mekanisme til at informere de relevante medlemsstaters kompetente myndigheder om en sådan viderebehandling af oplysninger[39]. Desuden bør det beskyttelsesniveau for fysiske personer, som er fastsat i Unionen i direktivet om retshåndhævelse, under alle omstændigheder ikke undermineres, herunder i de tilfælde af videreoverførsel af personoplysninger fra tredjelandet til dataansvarlige eller databehandlere i det samme tredjeland[40].

d) Særlige betingelser for viderebehandling til andre formål (artikel 9)

41. Hvad angår viderebehandling eller videregivelse af oplysninger, der er overført fra EU, til andre formål end retshåndhævelsesformål, såsom nationale sikkerhedsformål, bør disse også være fastsat ved lov, være nødvendige og forholdsmæssige. Der bør også tages hensyn til, at der findes en mekanisme til at informere de relevante medlemsstaters kompetente myndigheder om en sådan viderebehandling af oplysninger[41]. Også her bør oplysningerne, når de er viderebehandlet eller videregivet, være omfattet af det samme beskyttelsesniveau, som da de oprindeligt blev behandlet af den modtagende kompetente myndighed.

e) Dataminimeringsprincippet

42. De skal være tilstrækkelige, relevante og ikke for omfattende i forhold til de formål, hvortil de behandles. Navnlig bør der tages hensyn til anvendelsen af krav om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, såsom felter med begrænset adgang (strukturerede meddelelser) eller automatiserede og ikke-automatiserede kvalitetskontroller.

[36] Dette omfatter "politiaktiviteter uden forudgående viden om, hvorvidt et forhold udgør en strafbar handling eller ej. Sådanne aktiviteter kan også omfatte udøvelsen af beføjelser gennem tvangsindgreb som f.eks. politiaktiviteter i forbindelse med demonstrationer, store sportsbegivenheder og uroligheder. De omfatter også opretholdelse af lov og orden som en opgave, der er overdraget til politiet eller andre retshåndhævende myndigheder, hvor det er nødvendigt for at beskytte mod og forebygge trusler mod den offentlige sikkerhed og de ved lov beskyttede grundlæggende samfundsinteresser, som kan føre til en strafbar handling" (betragtning 12 i direktivet om retshåndhævelse). Der skal sondres mellem dette og et nationalt sikkerhedsformål eller aktiviteter, der falder inden for rammerne af afsnit V, kapitel 2, i traktaten om Den Europæiske Union (TEU) (betragtning 14 i direktivet om retshåndhævelse).
[37] Jf. fodnote 33.
[38] Betragtning 29 i direktivet om retshåndhævelse.
[39] En sådan mekanisme kunne f.eks. være gensidigt aftalte regler for behandling, en meddelelsespligt i henhold til et internationalt instrument, herunder eventuelle automatiske meddelelser, eller andre lignende gennemsigtighedsforanstaltninger.
[40] Betragtning 64 i direktivet om retshåndhævelse.
[41] Jf. fodnote 39.

f) Princippet om oplysningernes rigtighed

43. Oplysningerne bør være korrekte og om nødvendigt ajourførte. Princippet om oplysningernes rigtighed bør dog anvendes under hensyntagen til den pågældende behandlings karakter og formål. Navnlig i retssager er udsagn, der indeholder personoplysninger, baseret på en subjektiv opfattelse af fysiske personer, og det er ikke altid muligt at kontrollere dem. Kravet om oplysningernes rigtighed bør derfor ikke vedrøre et udsagns rigtighed, men blot det forhold, at der er fremsat et konkret udsagn[42].

44. Det bør sikres, at personoplysninger, som er urigtige, ufuldstændige eller ikke længere ajourførte, ikke videregives eller stilles til rådighed[43], og at der er planlagt procedurer til at rette eller slette ukorrekte oplysninger. Der bør navnlig tages hensyn til eventuelle klassificeringssystemer for de behandlede oplysninger med hensyn til kildens pålidelighed og med hensyn til kontrolniveauet[44] for fakta.

g) Datalagringsprincippet

45. Oplysninger bør ikke opbevares i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de behandles. Der bør indføres passende mekanismer til sletning af personoplysninger; det kan være en fast periode eller en periodisk gennemgang af behovet for lagring af personoplysninger (eller en kombination af begge: fastsat maksimumsperiode og periodisk revision med bestemte intervaller)[45]. Personoplysninger, der i længere perioder opbevares til arkivformål i samfundets interesse eller til videnskabelig, statistisk eller historisk brug, bør være omfattet af de fornødne garantier (f.eks. med hensyn til adgang)[46].

h) Princippet om sikkerhed og fortrolighed (artikel 29, betragtning 28 og 71)

46. Enhver enhed, der behandler personoplysninger, bør sikre, at oplysningerne behandles på en måde, der garanterer personoplysningernes sikkerhed, herunder ved at forhindre uautoriseret adgang til eller brug af personoplysninger og det udstyr, der anvendes til behandlingen. Dette omfatter beskyttelse mod og passende foranstaltninger til at håndtere ulovlig behandling samt hændeligt tab, ødelæggelse eller beskadigelse ved hjælp af passende tekniske og organisatoriske foranstaltninger. Ved fastlæggelsen af sikkerhedsniveauet bør der tages hensyn til det aktuelle tekniske niveau, gennemførelsesomkostningerne og behandlingens art, omfang, kontekst og formål samt risikoen af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

47. Der bør sikres sikre kommunikationskanaler mellem de myndigheder i medlemsstaterne, der overfører personoplysningerne, og tredjelandenes modtagende myndigheder.

i) Gennemsigtighedsprincippet (artikel 13, betragtning 26, 39, 42, 43, 44 og 46)

48. Fysiske personer bør gøres bekendt med risici, regler, garantier og rettigheder i forbindelse med behandling af deres personoplysninger og med, hvordan de skal udøve deres rettigheder i forbindelse med behandlingen[47].

[42] Betragtning 30 i direktivet om retshåndhævelse.
[43] Betragtning 32 i direktivet om retshåndhævelse.
[44] F.eks. 4x4 gitter til pålidelighedsvurderinger og regler for behandling.
[45] Artikel 5 i direktivet om retshåndhævelse.
[46] Betragtning 26 i direktivet om retshåndhævelse.
[47] Betragtning 26 i direktivet om retshåndhævelse.

49. Oplysninger om alle hovedelementerne i behandlingen af deres personoplysninger bør stilles til rådighed for de fysiske personer. Disse oplysninger bør være let tilgængelige og letforståelige i et klart og forståeligt sprog. Disse oplysninger skal omfatte formålet med behandlingen, den dataansvarliges identitet, de rettigheder, som den pågældende fysiske person har[48], samt andre oplysninger, der måtte være nødvendige af hensyn til rimeligheden.

50. Der kan være visse undtagelser fra denne ret til oplysninger. En sådan begrænsning bør dog være tilladt ved en lovgivningsmæssig foranstaltning og være nødvendig og forholdsmæssig for at undgå, at der lægges hindringer i vejen for officielle eller retlige undersøgelser, for at undgå, at forebyggelsen, efterforskningen, afsløringen eller retsforfølgningen af strafbare handlinger skades, eller af hensyn til fuldbyrdelsen af strafferetlige sanktioner, for at beskytte den offentlige sikkerhed eller den nationale sikkerhed eller beskytte andres rettigheder og frihedsrettigheder, så længe en sådan delvis eller fuldstændig begrænsning udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund under behørig hensyntagen til den pågældende fysiske persons grundlæggende rettigheder og legitime interesser. Sådanne begrænsninger bør også overvejes og vurderes under hensyntagen til muligheden for at indgive en klage til en tilsynsmyndighed eller søge et retsmiddel. Under alle omstændigheder bør enhver mulig begrænsning være midlertidig og ikke generel, og den bør være omfattet af betingelser, garantier og begrænsninger, der svarer til dem, der kræves i henhold til chartret og EMRK, som fortolket i henholdsvis EU-Domstolens og Menneskerettighedsdomstolens retspraksis, og bør navnlig respektere disse rettigheders og friheders væsentligste indhold.

j) Retten til indsigt, berigtigelse og sletning (artikel 14 og 16)

51. Den registrerede bør have ret til at få bekræftet, om behandlingen af personoplysninger vedrørende den pågældende finder sted, og i givet fald have adgang til sine oplysninger. Denne ret bør som minimum omfatte visse oplysninger om behandlingen, såsom formålene med og retsgrundlaget for behandlingen, retten til at indgive en klage til tilsynsmyndigheden eller de berørte kategorier af personoplysninger[49]. Dette er særlig vigtigt, hvis gennemsigtigheden opnås gennem generel meddelelse (f.eks. oplysninger på myndighedens websted).

52. Den registrerede bør have ret til at få berigtiget sine oplysninger af nærmere angivne årsager, f.eks. hvis det viser sig, at oplysningerne er urigtige eller ufuldstændige. Den registrerede bør også have ret til at få sine oplysninger slettet, f.eks. hvis behandlingen af dem ikke længere er nødvendig eller er ulovlig.

53. Udøvelsen af disse rettigheder bør ikke være overdrevent byrdefuld for den registrerede.

k) Begrænsninger i registreredes rettigheder

54. Der kan være begrænsninger i disse rettigheder for at undgå, at der lægges hindringer i vejen for officielle eller retlige undersøgelser, for at undgå, at forebyggelsen, efterforskningen, afsløringen eller retsforfølgningen af strafbare handlinger skades, eller af hensyn til fuldbyrdelsen af strafferetlige sanktioner, for at beskytte den offentlige sikkerhed eller den nationale sikkerhed eller beskytte andres rettigheder og frihedsrettigheder, så længe en sådan delvis eller fuldstændig begrænsning udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund under behørig hensyntagen til den pågældende fysiske persons grundlæggende rettigheder og

[48] Både materielle rettigheder (ret til indsigt, berigtigelse osv.) og klageadgang.
[49] Artikel 14 i direktivet om retshåndhævelse.

legitime interesser. Sådanne begrænsninger bør også overvejes og vurderes under hensyntagen til muligheden for at indgive en klage til en tilsynsmyndighed eller indbringe sagen for en domstol.

l) Begrænsning af videreoverførsel (artikel 35, betragtning 64-65)

55. Den oprindelige modtagers videreoverførsler af personoplysninger til et andet tredjeland eller en anden international organisation må ikke underminere det beskyttelsesniveau, der er fastsat i Unionen for fysiske personer, hvis oplysninger videregives. En sådan videreoverførsel af oplysninger bør derfor kun tillades, hvis kontinuiteten i det beskyttelsesniveau, der ydes i henhold til EU-retten, er sikret[50]. Navnlig bør den yderligere modtager (dvs. modtageren af videreoverførslen) være en kompetent myndighed med henblik på retshåndhævelse[51], og sådanne videreoverførsler af oplysninger må kun finde sted til begrænsede og nærmere angivne formål, og så længe der er et retligt grundlag for denne behandling.

56. Der skal også tages hensyn til, at der findes en mekanisme, der gør det muligt for den relevante medlemsstats kompetente myndigheder at blive underrettet om og tillade en sådan videreoverførsel af oplysninger. Den oprindelige modtager af de oplysninger, der overføres fra EU, bør være ansvarlig og kunne bevise, at den relevante kompetente myndighed i medlemsstaten har godkendt videreoverførslen[52], og at der er de fornødne garantier for videreoverførsel af oplysninger, hvis der ikke foreligger en afgørelse om tilstrækkeligheden af beskyttelsesniveauet vedrørende det tredjeland, hvortil oplysningerne videregives[53].

m) Ansvarlighedsprincippet (artikel 4, stk. 4)

57. Den dataansvarlige bør være ansvarlig for og i stand til at påvise overensstemmelse med databeskyttelsesprincipperne i artikel 4 i direktivet om databeskyttelse.

[50] Se også udtalelse 1/15.
[51] Jf. fodnote 33.
[52] I denne forbindelse bør der tages hensyn til, om der foreligger en forpligtelse til eller et tilsagn om at gennemføre relevante regler for behandling, som er fastlagt af de overførende medlemsstaters myndigheder.
[53] Ovenstående krav berører ikke de særlige betingelser for videreoverførsel til et passende land, der er fastsat i direktivet om retshåndhævelse (artikel 35, stk. 1, litra c) og e)).

B. Eksempler på yderligere principper, der skal anvendes på specifikke former for behandling

a) Særlige kategorier af oplysninger (artikel 10 og betragtning 37)

58. Der bør være særlige garantier, når der er tale om "særlige kategorier af oplysninger"[54], for så vidt angår de specifikke risici, der er forbundet hermed[55]. Disse kategorier bør afspejle dem, der er fastsat i artikel 10 i direktivet om retshåndhævelse. Behandling af særlige kategorier af oplysninger bør derfor være underlagt særlige garantier og kun tillades, hvis det er strengt nødvendigt på visse betingelser, f.eks. for at beskytte en persons vitale interesser.

b) Automatiseret beslutningstagning og profilering (artikel 11 og betragtning 38)

59. Afgørelser, der udelukkende er baseret på automatiseret behandling (automatiseret individuel beslutningstagning), herunder profilering, og som har negative retsvirkninger eller i væsentlig grad påvirker den registrerede, bør kun træffes på visse betingelser, der er fastsat i tredjelandets retlige ramme[56].

60. Inden for EU's rammer omfatter sådanne betingelser f.eks. udlevering af specifikke oplysninger til den registrerede og retten til menneskelig indgriben fra den dataansvarliges side, navnlig til at give udtryk for sine synspunkter, til at få en forklaring på den afgørelse, der er truffet efter en sådan vurdering, eller til at anfægte afgørelsen.

61. Tredjelandets lovgivning bør under alle omstændigheder indeholde de nødvendige garantier for den registreredes rettigheder og frihedsrettigheder. I denne forbindelse bør der også tages hensyn til, at der findes en mekanisme til at informere den relevante medlemsstats kompetente myndigheder om enhver yderligere behandling, såsom anvendelse af de overførte data til omfattende profilering.

c) Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger (artikel 20)

62. Ved vurderingen af tilstrækkeligheden bør der lægges vægt på, at de dataansvarlige har pligt til at vedtage interne politikker og gennemføre foranstaltninger, der overholder principperne om indbygget databeskyttelse og databeskyttelse gennem indstillinger, under hensyntagen til det aktuelle tekniske niveau, gennemførelsesomkostningerne og behandlingens art, omfang, kontekst og formål samt de risici af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, der er forbundet med behandlingen, både på tidspunktet for fastlæggelsen af midlerne til behandling og på tidspunktet for selve behandlingen af personoplysninger, således at der træffes passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, som er designet med henblik på implementering af databeskyttelsesprincipper, såsom dataminimering, på en effektiv måde, samt for at integrere de nødvendige sikkerhedsforanstaltninger i behandlingen.

[54] Sådanne særlige kategorier kaldes også "følsomme oplysninger" i betragtning 37 i direktivet om databeskyttelse.
[55] Sådanne yderligere sikkerhedsforanstaltninger kan f.eks. være specifikke sikkerhedsforanstaltninger, begrænsede adgangsrettigheder for personale, begrænsninger med hensyn til viderebehandling, automatiseret beslutningstagning, videredeling eller videreoverførsel.
[56] Udtalelse 1/15, præmis 173.

C. Procedure- og håndhævelsesmekanismer

63. Selv om de midler, som tredjelandet anvender for at sikre et tilstrækkeligt beskyttelsesniveau, kan være forskellige fra de midler, som gennemføres inden for EU[57], skal et system, der svarer til det europæiske system, være kendetegnet ved følgende elementer:

a) Kompetent uafhængig tilsynsmyndighed (artikel 36, stk. 2, litra b), og artikel 36, stk. 3, samt betragtning 67)

64. Der bør være en eller flere uafhængige tilsynsmyndigheder, som har til opgave at overvåge, sikre og håndhæve overholdelsen af bestemmelserne om databeskyttelse og beskyttelse af privatlivets fred i tredjelandet. Tilsynsmyndigheden handler fuldstændig uafhængigt og uvildigt ved udførelsen af sine opgaver og udøvelsen af sine beføjelser og skal hverken indhente eller acceptere instrukser. I den forbindelse bør tilsynsmyndigheden have alle tilstrækkelige håndhævelsesbeføjelser til effektivt at sikre overholdelse af databeskyttelsesrettigheder og øge bevidstheden herom. Der bør også tages hensyn til tilsynsmyndighedens personale og budget. Tilsynsmyndigheden skal også være i stand til at foretage undersøgelser på eget initiativ. Den bør også have til opgave at bistå og rådgive de registrerede i forbindelse med udøvelsen af deres rettigheder (se også punkt c nedenfor). Afgørelser om tilstrækkeligheden af beskyttelsesniveauet bør, hvor det er relevant, identificere den eller de pågældende tilsynsmyndigheder og samarbejdsmekanismerne med medlemsstaternes tilsynsmyndigheder med henblik på at håndhæve databeskyttelsesreglerne.

b) Effektiv gennemførelse af databeskyttelsesreglerne

65. Et system i et tredjeland bør sikre en høj grad af bevidsthed blandt de dataansvarlige og dem, der behandler personoplysninger på deres vegne, om deres forpligtelser, opgaver og ansvar, og blandt de registrerede om deres rettigheder og midlerne til at gøre disse rettigheder gældende. Tilstedeværelsen af effektive og afskrækkende sanktioner kan spille en vigtig rolle med hensyn til at sikre, at reglerne bliver overholdt, og det kan systemer med direkte kontrol fra myndighedernes, revisorers eller uafhængige databeskyttelsesembedsmænds side også.

66. Et tredjelands databeskyttelseslovgivning bør forpligte dataansvarlige og/eller dem, der behandler personoplysninger på deres vegne, til at overholde lovgivningen og til at kunne påvise en sådan overholdelse, navnlig over for den kompetente tilsynsmyndighed. Sådanne foranstaltninger bør omfatte opbevaring af registre eller logfiler over databehandlingsaktiviteter i et passende tidsrum. De kan f.eks. også omfatte konsekvensanalyser vedrørende databeskyttelse, udpegelse af en databeskyttelsesansvarlig eller databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

c) Databeskyttelsessystemet skal lette udøvelsen af registreredes rettigheder (artikel 12, 17 og 46 i direktivet om databeskyttelse)

67. Et tredjelands databeskyttelsesramme bør forpligte de registeransvarlige til at lette udøvelsen af registreredes rettigheder som omhandlet i afsnit A, litra j), ovenfor, og fastsætte, at tredjelandets tilsynsmyndighed efter anmodning skal informere enhver registreret om udøvelsen af deres rettigheder[58].

[57] Schrems I, præmis 74.
[58] Udøvelsen af registreredes rettigheder kan være enten direkte eller indirekte.

d) Databeskyttelsessystemet skal indeholde passende søgsmålsmekanismer

68. Selv om der i øjeblikket ikke findes nogen retspraksis vedrørende tilstrækkeligheden af et tredjelands retssystem i henhold til direktivet om retshåndhævelse, har EU-Domstolen fortolket den grundlæggende ret til effektiv domstolsbeskyttelse som fastsat i chartrets artikel 47. Chartrets artikel 47, stk. 1, opstiller et krav om, at enhver, hvis rettigheder og friheder som sikret af EU-retten er blevet krænket, skal have adgang til effektive retsmidler for en domstol[59] under overholdelse af de betingelser, der er fastsat i denne artikel.

69. Ifølge EU-Domstolens faste retspraksis er selve eksistensen af en effektiv domstolsbeskyttelse, som skal sikre overholdelsen af EU-retlige bestemmelser, uløseligt forbundet med eksistensen af en retsstat. En lovgivning, der ikke fastsætter nogen mulighed for retssubjektet til at gøre brug af retsmidler med henblik på at få adgang til personoplysninger, som vedrører den pågældende, eller til at få sådanne oplysninger berigtiget eller slettet, opfylder således ikke det væsentligste indhold af den grundlæggende ret til en effektiv domstolsbeskyttelse, således som den er sikret ved chartrets artikel 47[60].

70. Fysiske personer skal kunne gøre brug af retsmidler til at få håndhævet deres rettigheder hurtigt og effektivt og uden uforholdsmæssigt store omkostninger samt til at sikre overholdelse.

71. Det kræver, at der er indført tilsynsmekanismer, som muliggør uafhængig undersøgelse af klager og sikrer, at alle krænkelser af retten til databeskyttelse og respekt for privatlivets fred bliver identificeret og straffet i praksis.

72. Hvis reglerne ikke overholdes, bør den registrerede, hvis personoplysninger overføres til tredjelandet, også have adgang til effektive administrative og retlige klagemuligheder i tredjelandet, herunder mulighed for erstatning for skader som følge af ulovlig behandling af vedkommendes personoplysninger. Dette er et centralt element, som skal omfatte et system med uafhængig voldgift, der gør det muligt at få udbetalt erstatning og pålagt sanktioner, når dette er påkrævet.

[59] EU-Domstolen mener, at en effektiv retsbeskyttelse ikke udelukkende kan sikres af en domstol, men også af et organ, der tilbyder garantier, der i det væsentlige svarer til dem, der kræves i henhold til chartrets artikel 47 (jf. Schrems II, præmis 197). Dette kan især være relevant for internationale organisationer.
[60] Schrems II, præmis 187 og præmis 194, herunder citeret retspraksis.