Rekommendationer

Rekommendationer 01/2021 om referensramen för adekvat skyddsnivå enligt direktivet om uppgiftsskydd vid brottsbekämpning

Antagna den 2 februari 2021

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

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit dessa rekommendationer

med beaktande av artikel 51.1 b i Europarlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF[1], och

med beaktande av artiklarna 12 och 22 i arbetsordningen.

HÄRIGENOM REKOMMENDERAS FÖLJANDE

1. INLEDNING

1. Artikel 29-arbetsgruppen har offentliggjort ett arbetsdokument[2] om referensramen för adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen (*dataskyddsförordningen*)[3]. Europeiska dataskyddsstyrelsen (EDPB) godkände detta arbetsdokument vid sitt första plenarsammanträde.

2. Såsom anges i förklaring nr 21 som fogats till Lissabonfördraget kan det visa sig bli nödvändigt med särskilda regler om skydd av personuppgifter och om fri rörlighet för sådana uppgifter på områdena för straffrättsligt samarbete och polissamarbete, på grundval av artikel 16 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), på grund av de särskilda förhållanden som gäller på dessa områden.

3. Mot denna bakgrund har EU-lagstiftaren antagit direktiv (EU) 2016/680 (*direktivet om uppgiftsskydd vid brottsbekämpning*) som fastställer särskilda bestämmelser om behandling av personuppgifter som utförs av behöriga myndigheter i syfte att **förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten**.

4. I detta direktiv fastställs de grunder på vilka överföring av personuppgifter till ett tredjeland eller en internationell organisation är tillåten i detta sammanhang. En av grunderna för en sådan överföring är ett beslut från kommissionen att tredjelandet eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå.

5. Arbetsdokument WP254.rev01 om referensramen för adekvat skyddsnivå har till syfte att vägleda kommissionen om skyddsnivåer för personuppgifter i tredjeländer och internationella

[1] EUT L 119, 4.5.2016, s. 89.
[2] WP254.rev01 som antogs av artikel 29-arbetsgruppen den 28 november 2017, senast reviderat och antaget den 6 februari 2018. Det uppdaterar kapitel I i arbetsdokumentet *Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv*, WP12 som artikel 29-arbetsgruppen antog den 24 juli 1998.
[3] Europaparlamentets och rådets förordning (EU) 2016/679 av den 26 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

organisationer inom ramen för dataskyddsförordningen, medan detta dokument syftar till att ge liknande vägledning inom ramen för direktivet om uppgiftsskydd vid brottsbekämpning. I detta sammanhang fastställer det de grundprinciper för dataskydd som måste finnas i ett tredjelands eller en internationell organisations rättsliga ram för att väsentlig likvärdighet ska uppnås med EU:s rättsliga ramar inom tillämpningsområdet för direktivet om uppgiftsskydd vid brottsbekämpning (t.ex. vid behandling av personuppgifter från behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder). Därutöver kan dokumentet fungera som vägledning för tredjeländer och internationella organisationer som är intresserade av att uppnå en adekvat skyddsnivå.

6. Fokus i detta dokument ligger enbart på beslut om adekvat skyddsnivå. Dessa utgörs av genomförandeakter från kommissionen enligt artikel 36.3 i direktivet om uppgiftsskydd vid brotts-bekämpning.

2. BEGREPPET ADEKVAT SKYDDSNIVÅ

7. I direktivet om uppgiftsskydd vid brottsbekämpning fastställs bestämmelser för överföring av personuppgifter till tredjeländer och internationella organisationer i den utsträckning sådana överföringar omfattas av dess tillämpningsområde. Bestämmelserna om internationella överföringar av personuppgifter föreskrivs i kapitel V i direktivet, särskilt i artiklarna 35–39.

8. Enligt artikel 36 i direktivet får personuppgifter överföras till ett tredjeland eller en internationell organisation om tredjelandet, ett territorium eller en eller flera specificerade sektorer inom tredjelandet eller den internationella organisationen säkerställer en adekvat skyddsnivå. Det framgår av EU-domstolens rättspraxis[4] att denna artikel ska läsas mot bakgrund av artikel 35 i direktivet om uppgiftsskydd vid brottsbekämpning, med rubriken Allmänna principer för överföringar av personuppgifter. Där föreskrivs att ”[a]lla bestämmelser [i kapitel V i direktivet] ska tillämpas för att säkerställa att den skyddsnivå för fysiska personer som säkerställs genom detta direktiv inte undergrävs”.

9. Om kommissionen har beslutat att en sådan adekvat skyddsnivå är säkerställd får personuppgifter överföras till detta tredjeland eller territorium eller denna sektor eller internationella organisation utan att det krävs något särskilt tillstånd, utom när en annan medlemsstat från vilken uppgifterna insamlades måste ge tillstånd till överföringen såsom föreskrivs i artiklarna 35 och 36 och skäl 66 i direktivet om uppgiftsskydd vid brottsbekämpning. Detta påverkar inte skyldigheten för myndigheter i berörda medlemsstater att följa de nationella bestämmelser som har antagits i enlighet med direktiv (EU) 2016/680.

10. EU-domstolen har vidareutvecklat begreppet ”adekvat skyddsnivå” som fanns med redan i direktiv 95/46[5] och i rådets rambeslut 2008/977/RIF[6], i detta sammanhang och nyligen inom ramen för dataskyddsförordningen.

[4] Mål C-311/18, Data Protection Commissioner/Facebook Ireland Ltd och Maximillian Schrems, 16 juli 2020, ECLI:EU:C:2020:559, punkt 92 (Schrems II).
[5] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, EGT L 281, 23.11.1995, s. 31.
[6] Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, EUT L 350, 30.12.2008, s. 60.

11. EU-domstolen har specificerat att medan skyddsnivån i tredjelandet måste vara väsentligen likvärdig med den som garanteras inom EU gäller att ”de medel som detta tredjeland använder för att säkerställa en sådan skyddsnivå kan skilja sig från dem som används inom unionen”, men att ”dessa medel dock [måste] visa sig i praktiken kunna säkerställa ett skydd som är väsentligen likvärdigt”[7]. Därför måste standarden för adekvat skyddsnivå inte punkt för punkt efterlikna EU-lagstiftningen utan ska fastställa de grundläggande och avgörande kraven i denna lagstiftning.

12. I detta sammanhang har domstolen även klargjort att ett beslut om adekvat skyddsnivå från kommissionen inte bör innehålla något konstaterande beträffande förekomsten i tredjelandet av regler som detta land antagit och som syftar till att begränsa eventuella ingrepp i de grundläggande rättigheterna för personer vilkas personuppgifter överförs från unionen till detta tredjeland, ingrepp som offentliga organ kan vara *tillåtna* att göra när de görs i ett legitimt syfte, såsom nationell säkerhet[8].

13. Syftet med kommissionens beslut om adekvat skyddsnivå är att formellt bekräfta, med bindande verkan för medlemsstaterna[9], inbegripet deras behöriga dataskyddsmyndigheter[10], att skyddsnivån för personuppgifter i ett tredjeland eller en internationell organisation är väsentligen likvärdig med skyddsnivån för personuppgifter i EU. Tredjelandet bör erbjuda garantier som säkerställer en tillfredsställande skyddsnivå, som i huvudsak motsvarar den som säkerställs inom unionen, i synnerhet när uppgifter behandlas inom en eller flera specifika sektorer[11].

14. Adekvat skyddsnivå kan uppnås genom en kombination av rättigheter för de registrerade och skyldigheter för de som behandlar personuppgifter, eller som utövar kontroll över sådan behandling, och övervakning av oberoende organ. Bestämmelser om skydd av personuppgifter är dock endast effektiva om de är verkställbara och följs i praktiken. Det är därför nödvändigt att inte bara se till innehållet i bestämmelserna för överföring av personuppgifter till ett tredjeland eller en internationell organisation utan också till de mekanismer som har inrättats för att säkerställa att dessa bestämmelser är verkningsfulla. Effektiva verkställighetsmekanismer är av avgörande betydelse för att få effektiva bestämmelser om skydd av personuppgifter[12].

3. FÖRFARANDEN GÄLLANDE BEDÖMNINGAR OM ADEKVAT SKYDDSNIVÅ INOM RAMEN FÖR DIREKTIVET OM UPPGIFTSSKYDD VID BROTTSBEKÄMPNING

15. För att EDPB ska kunna fullgöra sin uppgift att lämna råd till kommissionen enligt artikel 51.1 g i direktivet om uppgiftsskydd vid brottsbekämpning ska den erhålla all relevant dokumentation,

[7] Mål C-362/14, Maximillian Schrems/Data Protection Commissioner, 6 oktober 2015, ECLI:EU:C:2015:650, punkterna 73 och 74 (Schrems I).
[8] Schrems I, punkt 88.
[9] Artikel 288.2 i EUF-fördraget.
[10] Schrems I, punkt 52.
[11] Skäl 67 i direktivet om uppgiftsskydd vid brottsbekämpning.
[12] Schrems I, punkterna 72–74 och EU-domstolens yttrande 1/15 om förslaget till avtal mellan Kanada och Europeiska unionen, 26 juli 2017, ECLI:EU:C:2017:592 (yttrande 1/15), punkt 134: ”Rätten till skydd av personuppgifter kräver bland annat att den höga nivå för skydd av grundläggande fri- och rättigheter som följer av unionsrätten vidmakthålls vid överföring av personuppgifter från unionen till ett tredjeland. Även om de medel som detta tredjeland använder för att säkerställa en sådan skyddsnivå kan skilja sig från dem som används inom unionen för att säkerställa iakttagandet av de krav som följer av unionsrätten måste dessa medel dock visa sig i praktiken kunna säkerställa ett skydd som är väsentligen likvärdigt med det skydd som garanteras inom unionen.”

inklusive relevant korrespondens och de bedömningar som gjorts av kommissionen. Det är absolut nödvändigt att alla relevanta dokument överförs till EDPB i tillräckligt god tid och översätts till engelska för att möjliggöra väl underbyggda och givande diskussioner innan ett slutgiltigt beslut om adekvat skyddsnivå antas. I de fall då den rättsliga ramen är komplex bör eventuella rapporter som tagits fram om skyddsnivån för uppgifter i tredjelandet eller den internationella organisationen innefattas. Under alla omständigheter ska informationen som lämnas av kommissionen vara uttömmande och göra det möjligt för EDPB att göra en bedömning av kommissionens analys av skyddsnivån för personuppgifter i tredjelandet eller i den internationella organisationen.

16. EDPB ska avge ett yttrande om kommissionens bedömningar inom utsatt tid och identifiera eventuella brister i den rättsliga ramen för adekvat skyddsnivå samt vid behov lämna eventuella rekommendationer.

17. Enligt artikel 36.4 i direktivet om uppgiftsskydd vid brottsbekämpning är kommissionen skyldig att fortlöpande övervaka utveckling som kan påverka hur beslut om adekvat skyddsnivå fungerar.

18. I artikel 36.3 i direktivet fastställs att en regelbunden översyn måste utföras minst vart fjärde år. Detta ska dock betraktas som en generell tidsram som måste anpassas för varje tredjeland eller internationell organisation som omfattas av ett beslut om adekvat skyddsnivå. Beroende på de specifika omständigheter som råder kan det krävas att översynen utförs med tätare intervall. Dessutom kan incidenter eller annan information om eller ändringar i den rättsliga ramen för tredjelandet eller den internationella organisationen i fråga vara grund för att utföra en översyn tidigare än planerat. Det förefaller även lämpligt att ha en första översyn av ett helt nytt beslut om adekvat skyddsnivå relativt tidigt, och att sedan gradvis justera översynsintervallen utifrån resultatet.

19. Med tanke på uppdraget att avge ett yttrande till kommissionen huruvida ett tredjeland, ett territorium eller en eller flera specificerade sektorer i tredjelandet eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå, måste EDPB, inom utsatt tid, erhålla meningsfull information om övervakningen av den relevanta utvecklingen i tredjelandet eller den internationella organisationen från kommissionen. Av den anledningen bör EDPB hållas underrättad om eventuella översynsprocesser och översynsuppdrag i tredjelandet eller gällande den internationella organisationen. EDPB rekommenderar att den bjuds in att delta i dessa översynsprocesser och översynsuppdrag, såsom föreskrivs i beslutet om skölden för skydd av privatlivet (*Privacy Shield*) och beslutet om adekvat skyddsnivå beträffande Japan.

20. Det ska även noteras att kommissionen enligt artikel 36.5 i direktivet om uppgiftsskydd vid brottsbekämpning har behörighet att dra tillbaka, ändra eller upphäva befintliga beslut om adekvat skyddsnivå när ett tredjeland eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå. EDPB är involverad i förfarandet för att dra tillbaka, ändra eller upphäva beslut, genom att dess yttrande ska inhämtas enligt artikel 51.1 g i direktivet.

21. Vidare bör tillsynsmyndigheterna, utan att det påverkar åklagarmyndigheternas befogenheter, också ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av detta direktiv eller inleda rättsliga förfaranden[13]. Det framgår framför allt av EU-domstolens dom i målet Schrems I att dataskyddsmyndigheter ska kunna inleda rättsliga förfaranden vid nationella

[13] Se artikel 47.5 i direktivet om uppgiftsskydd samt skäl 82 i nämnda direktiv.

domstolar om de finner att en persons anspråk gentemot ett beslut om adekvat skyddsnivå är välgrundat[14]. Denna bedömning bekräftades i domen i målet Schrems II[15].

4. EU:S STANDARDER FÖR ADEKVAT SKYDDSNIVÅ VID POLISSAMARBETE OCH STRAFFRÄTTSLIGT SAMARBETE

22. I materiellt hänseende bör beslut om adekvat skyddsnivå inriktas på en såväl teoretisk som praktiskt bedömning av den befintliga lagstiftningen i det aktuella tredjelandet som helhet mot bakgrund av de bedömningskriterier som föreskrivs i artikel 36 i direktivet om uppgiftsskydd vid brottsbekämpning. Ett tredjelands eller en internationell organisations system måste innehålla följande grundläggande allmänna principer för skydd av personuppgifter och förfarande- och verkställandemekanismer.

23. I artikel 36.2 i direktivet fastställs de element som kommissionen ska beakta vid bedömningen av om en adekvat skyddsnivå föreligger i ett tredjeland eller en internationell organisation.

24. Kommissionen ska i synnerhet beakta rättsstatsprincipen, respekten för de mänskliga rättigheterna och grundläggande friheterna[16], relevant lagstiftning, liksom tillämpningen av sådan lagstiftning, effektiva och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs, huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet och vilka internationella åtaganden tredjelandet eller den internationella organisationen har gjort.

25. Det står således klart att en analys av vad som är en adekvat skyddsnivå endast blir meningsfull om den beaktar följande två grundläggande element: innehållet i de gällande bestämmelserna och instrumenten för att säkerställa att dessa tillämpas på ett effektivt sätt. Det ligger på kommissionens ansvar att regelbundet kontrollera att de bestämmelser som finns är effektiva i praktiken.

---

[14] Se Schrems I, punkt 65: ”Det ankommer härvidlag på den nationella lagstiftaren att föreskriva rättsmedel som gör det möjligt för den nationella tillsynsmyndigheten att vid nationella domstolar göra gällande de invändningar som den anser att det finns fog för, så att nationella domstolar, för det fall att de delar myndighetens tvivel angående kommissionsbeslutets giltighet, kan hänskjuta en begäran om förhandsavgörande för att pröva detta besluts giltighet.”

[15] Se Schrems II, punkt 120: ”Även när det föreligger ett kommissionsbeslut om adekvat skyddsnivå ska den behöriga nationella tillsynsmyndigheten – till vilken en person har ingett klagomål angående skyddet för sina fri- och rättigheter med avseende på behandlingen av personuppgifter som rör honom eller henne – kunna göra en fullständigt oberoende prövning av huruvida överföringen av uppgifterna uppfyller de krav som uppställs i dataskyddsförordningen och, i förekommande fall, inleda ett förfarande vid nationella domstolar i syfte att dessa domstolar, om de delar myndighetens tvivel angående giltigheten av beslutet om adekvat skydd, ska kunna hänskjuta en begäran om förhandsavgörande för att få beslutets giltighet prövad.”

[16] Vid bedömningen av tredjelandets rättsliga ram ska möjligheten att dödsstraff eller någon form av grym och omänsklig behandling åläggs på grundval av uppgifter som överförts från EU beaktas. Om det föreskrivs ett sådant straff eller en sådan behandling i tredjelandets lagstiftning bör det finnas ytterligare garantier i tredjelandets rättsliga ram för att säkerställa att uppgifter som överförts från EU inte används för att begära, meddela eller verkställa ett dödsstraff eller någon annan form av grym och omänsklig behandling (t.ex. ett internationellt avtal som ålägger villkor för överföringen, ett åtagande från tredjelandet att inte ålägga dödsstraff eller någon annan form av grym och omänsklig behandling på grundval av uppgifter som överförts från EU eller ett moratorium för dödsstraff).

26. Själva kärnan vad gäller allmänna principer för skydd av personuppgifter och krav i fråga om förfarande- och verkställandemekanismer, som kan ses som ett minimikrav för att skyddet ska vara adekvat, erhålls från EU:s stadga om de grundläggande rättigheterna (*stadgan*) och direktivet om uppgiftsskydd vid brottsbekämpning. Allmänna bestämmelser om uppgiftsskydd och integritetsskydd i tredjelandet är inte tillräckliga. Tvärtom måste specifika bestämmelser som konkret behandlar rätten till uppgiftsskydd inom området för brottsbekämpning ingå i tredjelandets eller den internationella organisationens rättsliga ram. Tredjelandet bör erbjuda garantier som säkerställer en tillfredsställande skyddsnivå, som i huvudsak motsvarar den som säkerställs inom unionen. Dessa bestämmelser måste vara verkställbara.

27. Vidare fann EU-domstolen med avseende på proportionalitetsprincipen[17], i förhållande till medlemsstaternas lagstiftning, att frågan huruvida en begränsning av rätten till integritet och dataskydd kan vara motiverad måste bedömas dels genom att bedöma hur **allvarligt det ingrepp** är som en sådan begränsning medför[18], dels genom att kontrollera att **betydelsen av det mål av allmänt samhällsintresse** som eftersträvas med denna begränsning står i proportion till hur allvarligt ingreppet är[19].

28. Enligt EU-domstolens rättspraxis måste en rättslig grund som gör ingreppet i de grundläggande rättigheterna möjligt – för att uppfylla kraven enligt proportionalitetsprincipen – i sig definiera räckvidden av begränsningen i utövandet av den aktuella rättigheten[20]. Undantag från och inskränkningar i skyddet av personuppgifter ska begränsas till vad som är strikt nödvändigt[21]. För att uppfylla detta krav måste den aktuella lagstiftning som innebär ett ingrepp innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden och fastställa minimikrav, så att de personer vilkas uppgifter har överförts har tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk. ”Lagstiftningen måste i synnerhet precisera under vilka omständigheter och på vilka villkor en åtgärd för behandling av personuppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strikt nödvändigt. Nödvändigheten av sådana garantier är av än större betydelse när personuppgifterna är föremål för automatisk behandling”[22].

29. EDPB har antagit rekommendationer som identifierar nödvändiga garantier som återspeglar rättspraxis från EU-domstolen och Europadomstolen inom området för övervakning som återfinns i tredjelandets lagstiftning vid bedömningen av ingrepp från sådana övervakningsåtgärder från tredjeländer i registrerades rättigheter om uppgifterna överförs till detta tredjeland enligt dataskyddsförordningen[23]. För att bedöma huruvida villkoren i artikel 36.2 i direktivet om uppgiftsskydd vid brottsbekämpning är uppfyllda anser EDPB att de garantier som föreskrivs i dessa rekommendationer ska beaktas vid bedömningen huruvida ett tredjeland har en adekvat skyddsnivå enligt direktivet inom området för övervakning, med hänsyn till ytterligare särskilda villkor inom övervakningsområdet i detta sammanhang.

---

[17] Artikel 52.1 i stadgan.

[18] Domstolen noterade till exempel att ”det ingrepp som en insamling i realtid av uppgifter som gör det möjligt att lokalisera en terminalutrustning innebär är synnerligen allvarligt, eftersom dessa uppgifter gör det möjligt för behöriga nationella myndigheter att exakt och varaktigt bevaka mobiltelefonanvändarnas förflyttningar …” (förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl., 6 oktober 2020, ECLI:EU:C:2020:791, punkt 187 och där angiven rättspraxis).

[19] La Quadrature du Net m.fl., punkt 131.

[20] Schrems II, punkt 180.

[21] Schrems II, punkt 176 och där angiven rättspraxis.

[22] Schrems II, punkt 176 och där angiven rättspraxis.

[23] EDPB:s rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder, antagna den 10 november 2020.

30. I förhållande till kravet i artikel 36.2 b bör tredjelandet inte bara säkerställa att övervakningen av uppgiftsskyddet är effektiv och oberoende, utan även sörja för mekanismer för samarbete med medlemsstaternas dataskyddsmyndigheter[24].

31. Vad gäller kravet i artikel 36.2 c ska, utöver de internationella åtaganden som tredjelandet eller den internationella organisationen har ingått, även skyldigheter som följer av tredjelandets eller den internationella organisationens deltagande i multilaterala eller regionala system beaktas, särskilt rörande skydd av personuppgifter, samt genomförandet av dessa skyldigheter, och framför allt tredjelandets anslutning till andra internationella avtal om dataskydd, t.ex. Europarådets konvention av den 28 januari 1981 om skydd för fysiska personer vid automatiserad databehandling av personuppgifter och dess tilläggsprotokoll (konvention 108[25] och dess moderniserade version, konvention 108+). Dessutom kan även tredjelandets iakttagande av principer som fastställs i internationella dokument såsom Europarådets *Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime* beaktas.

32. Genom ett beslut om adekvat skyddsnivå bör säkerställas att det utländska systemet som helhet tillhandahåller den skyddsnivå som krävs, inbegripet för uppgifter som överförs till detta land, genom de sammantagna rättigheter som föreligger när det gäller integritet och uppgiftsskydd och deras effektiva genomförande, tillsyn och verkställighet. Såsom EU-domstolen har framhållit i domen i målet Schrems II, ska den höga skyddsnivån även säkerställas medan uppgifter överförs till ett tredjeland[26].

33. Slutligen bör kommissionen vid antagandet av ett beslut om adekvat skyddsnivå som endast berör ett territorium eller en specificerad sektor i ett tredjeland ta hänsyn till tydliga och objektiva kriterier, såsom att hänvisa till specifik behandling och tillämpningsområdet för tillämpliga rättsliga standarder och gällande lagstiftning i det tredjelandet[27].

A. Allmänna principer och skyddsåtgärder

a) Begrepp

34. Grundläggande begrepp rörande skydd av personuppgifter bör vara definierade. Dessa begrepp behöver inte exakt återspegla terminologin i direktivet om uppgiftsskydd vid brottsbekämpning, men de bör avspegla och överensstämma med de begrepp som används i EU:s dataskydds-lagstiftning. Till exempel innehåller direktivet följande viktiga begrepp: ”personuppgifter”, ”behandling av personuppgifter”, ”behöriga myndigheter”, ”personuppgiftsansvarig”, ”person-uppgiftsbiträde”, ”mottagare”, ”känsliga uppgifter”, ”korrekthet”, ”profilering”, ”inbyggt data-skydd och dataskydd som standard”, ”tillsynsmyndighet” och ”pseudonymisering”.

b) Laglig och korrekt behandling av personuppgifter (artikel 4 – skäl 26)

35. Enligt artikel 8.2 i stadgan ska personuppgifter bland annat behandlas ”för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig

[24] Skäl 67 i direktivet om uppgiftsskydd vid brottsbekämpning.
[25] Skäl 68 i direktivet om uppgiftsskydd vid brottsbekämpning.
[26] Se punkt 93.
[27] Skäl 67 i direktivet om uppgiftsskydd vid brottsbekämpning.

grund”[28]. I samband med brottsbekämpning ska det emellertid noteras att fullgörandet av uppgifterna att förebygga, förhindra, utreda, avslöja eller lagföra brott som myndigheterna ålagts genom lag ger dem behörighet att kräva eller förelägga fysiska personer att följa framställningar som görs. I sådana situationer ska den registrerades samtycke inte utgöra rättslig grund för de behöriga myndigheternas behandling av personuppgifter[29].

36. Denna rättsliga grund bör innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella behandlingen av personuppgifter samt fastställer minimikrav[30]. Vidare har EU-domstolen erinrat om att ”lagstiftning ska vara rättsligt bindande enligt nationell rätt”[31].

37. För att vara laglig ska uppgiftsbehandlingen[32] vara nödvändig för att en behörig myndighet ska kunna utföra en uppgift i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten[33]. Syftet ska föreskrivas i nationell rätt.

38. Personuppgifter ska behandlas på ett korrekt sätt. Uppgiftsskyddsprincipen om korrekt behandling är ett begrepp som är skilt från rätten till en opartisk domstol enligt definitionen i artikel 47 i stadgan och rätten till en rättvis rättegång enligt definitionen i artikel 6 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (*Europakonventionen*)[34].

c) Principen om ändamålsbegränsning (artikel 4)

39. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in[35].

40. Uppgifter ska behandlas för ett särskilt, uttryckligt angivet och berättigat ändamål i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder[36],

---

[28] Se Schrems II, punkt 173.

[29] I skäl 35 i direktivet om uppgiftsskydd vid brottsbekämpning anges även följande: ”Om den registrerade är skyldig att fullgöra en rättslig förpliktelse har den registrerade inte någon genuin och fri valmöjlighet, och således är det inte möjligt att betrakta den registrerades reaktion som en frivillig viljeyttring. Detta bör inte hindra medlemsstaterna från att i lag fastställa att den registrerade får tillåta behandling av sina personuppgifter vid tillämpning av detta direktiv, såsom DNA-testning inom ramen för brottsutredningar eller övervakning av var den registrerade befinner sig med elektronisk fotboja för verkställighet av straffrättsliga påföljder”.

[30] Se Schrems II, punkterna 175 och 180 och yttrande 1/15, punkt 139 och där angiven rättspraxis.

[31] Se mål C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs m.fl, 6 oktober 2020, ECLI:EU:C:2020:790, punkt 68. Det ska även påpekas att EU-domstolen i den franska versionen av domen använder ordet ”réglementation”, vilket omfattar mer än enbart nationella lagar.

[32] Behandling av personuppgifter som helt eller delvis företas på automatisk väg samt annan behandling än automatisk av sådana personuppgifter som ingår i eller är avsedda att ingå i ett register.

[33] Med behörig myndighet avses en offentlig myndighet som är behörig för sådana ändamål eller annat organ eller annan enhet som genom lag har anförtrotts myndighetsutövning för sådana ändamål.

[34] Skäl 26 i direktivet om uppgiftsskydd vid brottsbekämpning.

[35] Skäl 26 i direktivet om uppgiftsskydd vid brottsbekämpning.

[36] Detta omfattar ”polisverksamhet där man inte på förhand vet om det inträffade utgör ett brott eller inte. Sådan verksamhet kan också innefatta myndighetsutövning genom vidtagande av tvångsåtgärder vid demonstrationer, större idrottsevenemang och upplopp. Denna verksamhet omfattar också upprätthållande av lag och ordning som en uppgift som anförtros åt polisen eller andra brottsbekämpande myndigheter när det är nödvändigt för att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och mot i lag skyddade grundläggande allmänna intressen som kan leda till ett brott” (skäl 12 i direktivet om uppgiftsskydd vid brottsbekämpning). Den

inklusive att skydda mot eller förebygga hot mot den allmänna säkerheten inom det tredje landet. De får därefter användas för samma ändamål om det inte är oförenligt med det ursprungliga syftet med behandlingen (t.ex. för parallella verkställighetsförfaranden eller arkivering av allmänt intresse eller vetenskaplig, statistisk eller historisk användning i sådana syften) och bör omfattas av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter. Om samma eller en annan personuppgiftsansvarig (behörig myndighet[37]) behandlar personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder som inte är det ändamål för vilket uppgifterna samlades in, bör behandlingen vara tillåten, förutsatt att behandlingen har godkänts i enlighet med tillämpliga rättsliga bestämmelser och är nödvändig och står i proportion till det andra ändamålet[38]. Det ska även beaktas om det finns en mekanism för att informera de relevanta medlemsstaternas behöriga myndigheter om sådan ytterligare behandling[39]. Det är vidare viktigt att den skyddsnivå som fysiska personer garanteras inom unionen genom direktivet inte undergrävs när personuppgifter överförs från tredjelandet till personuppgiftsansvariga eller personuppgiftsbiträden i samma tredjeland[40].

d) Särskilda villkor för ytterligare behandling för andra ändamål (artikel 9)

41. Vad gäller ytterligare behandling eller utlämnande av uppgifter som överförts från EU för andra ändamål än brottsbekämpning, såsom nationell säkerhet, krävs det att den även föreskrivs i lag samt är nödvändig och proportionerlig. Det ska även beaktas om det finns en mekanism för att informera de relevanta medlemsstaternas behöriga myndigheter om sådan ytterligare behandling[41]. Även här gäller att uppgifterna, så snart de behandlas ytterligare eller lämnas ut, ska åtnjuta samma skyddsnivå som när de ursprungligen behandlades av den mottagande behöriga myndigheten.

e) Principen om uppgiftsminimering

42. Uppgifterna vara adekvata, relevanta och inte mer omfattande än vad som krävs för de ändamål för vilka de behandlas. Tillämpning av krav på inbyggt dataskydd och dataskydd som standard, såsom begränsade inmatningsfält (strukturerad kommunikation) eller automatiska och icke-automatiska kvalitetskontroller ska särskilt beaktas.

f) Principen om uppgifternas korrekthet

43. Uppgifterna ska vara korrekta och, när så är nödvändigt, hållas aktuella. Principen om att uppgifter ska vara korrekta bör emellertid tillämpas med hänsyn till den typ av behandling det är fråga om och syftet med denna. Särskilt i domstolsförfaranden baseras utsagor som innehåller personuppgifter på fysiska personers subjektiva uppfattning, och kan inte alltid verifieras. Följaktligen bör inte korrekthetskravet röra korrektheten i en utsaga, utan endast det faktum att en viss utsaga har gjorts[42].

---

ska skiljas från verksamhet som rör nationell säkerhet eller verksamhet som omfattas av del V kapitel 2 i fördraget om Europeiska unionen (EU-fördraget) (skäl 14 i direktivet om uppgiftsskydd vid brottsbekämpning).

[37] Se fotnot 33.

[38] Skäl 29 i direktivet om uppgiftsskydd vid brottsbekämpning.

[39] Sådana mekanismer kan exempelvis utgöras av ömsesidigt avtalade hanteringskoder, en anmälningsskyldighet enligt ett internationellt instrument, inbegripet eventuella automatiska meddelanden, eller andra liknande åtgärder för insyn.

[40] Skäl 64 i direktivet om uppgiftsskydd vid brottsbekämpning.

[41] Se fotnot 39.

[42] Skäl 30 i direktivet om uppgiftsskydd vid brottsbekämpning.

44. Det bör säkerställas att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga[43] samt att förfaranden föreskrivs för att korrigera eller radera felaktiga uppgifter. I synnerhet ska man ta hänsyn till eventuella system för att klassificera den information som behandlas med avseende på hur tillförlitlig källan är samt på vilken nivå fakta verifieras[44].

g) Principen om lagring av uppgifter

45. Uppgifter ska inte bevaras under längre tid än vad som krävs för de ändamål för vilka de behandlas. Lämpliga mekanismer bör införas för radering av personuppgifter. Dessa kan bestå av en bestämd tidsperiod eller en periodisk översyn av behovet av att lagra personuppgifter (eller en kombination av båda med en bestämd maximal tidsperiod och en periodisk översyn med regelbundna mellanrum)[45]. Lämpliga skyddsåtgärder (t.ex. beträffande åtkomst) bör inrättas för personuppgifter som lagras under längre perioder, för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål)[46].

h) Principen om säkerhet och konfidentialitet (artikel 29, skälen 28 och 71)

46. Varje enhet som behandlar personuppgifter ska se till att uppgifterna behandlas på ett sätt som säkerställer personuppgifternas säkerhet, inbegripet genom att förhindra obehörigt tillträde till, eller obehörig användning av, personuppgifter och den utrustning som används för behandlingen. Detta omfattar skydd mot och lämpliga åtgärder för att hantera otillåten behandling samt förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder. Vid fastställandet av säkerhetsnivån ska den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter beaktas.

47. Det ska säkerställas att kommunikationskanalerna är säkra mellan de myndigheter i medlemsstaterna som överför personuppgifterna och mottagande myndigheter i tredje stater.

i) Öppenhetsprincipen (artikel 13, skälen 26, 39, 42, 43, 44, 46)

48. Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen[47].

49. Enskilda ska erhålla information om alla centrala delar av behandlingen av deras personuppgifter. Denna information ska vara lättåtkomlig och lättbegriplig, på ett klart och tydligt språk. Informationen ska ange ändamålet med behandlingen, den personuppgiftsansvariges identitet, individens rättigheter[48] och övrig information som krävs för att säkerställa en rättvis behandling.

50. Det kan förekomma vissa undantag från denna rätt till information. Sådana begränsningar ska emellertid grundas på lagstiftningsåtgärder och vara nödvändiga och proportionerliga för att

[43] Skäl 32 i direktivet om uppgiftsskydd vid brottsbekämpning.
[44] T.ex. 4x4-nät för tillförlitlighetsbedömningar och hanteringskoder.
[45] Artikel 5 i direktivet om uppgiftsskydd vid brottsbekämpning.
[46] Skäl 26 i direktivet om uppgiftsskydd vid brottsbekämpning.
[47] Skäl 26 i direktivet om uppgiftsskydd vid brottsbekämpning.
[48] Både de konkreta rättigheterna (rätt till tillgång, till rättelse etc.) och rätt till prövning.

undvika att officiella eller rättsliga utredningar, undersökningar eller förfaranden hindras, för att undvika menlig inverkan på förebyggande, förhindrande, utredning, upptäckt eller lagföring av brott eller verkställighet av straffrättsliga påföljder, för att skydda allmän eller nationell säkerhet eller för att skydda andra personers rättigheter och friheter så länge en sådan partiell eller fullständig begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med vederbörlig hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen. Sådana begränsningar bör även beaktas och bedömas med hänsyn till möjligheten att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning. I vart fall krävs det att alla eventuella begränsningar ska vara tillfälliga och inte allmänt utformade samt bygga på liknande villkor, säkerhetsåtgärder och begränsningar som de som krävs enligt stadgan och Europakonventionen, såsom de tolkas i EU-domstolens, respektive Europadomstolens, rättspraxis, särskilt vad gäller kärnan i dessa rättigheter och friheter.

j) Rätten till tillgång, rättelse och radering (artiklarna 14 och 16)

51. Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse av huruvida uppgifter som rör honom eller henne behandlas och i så fall få tillgång till sina uppgifter. Denna rätt ska åtminstone innehålla viss information om behandlingen, såsom ändamålen med behandlingen och dess rättsliga grund, rätten att lämna in klagomål till tillsynsmyndigheten eller de kategorier av personuppgifter som behandlingen gäller[49]. Detta är särskilt viktigt om öppenhet ska uppnås genom ett allmänt tillkännagivande (t.ex. information på myndighetens webbplats).

52. Den registrerade ska ha rätt att få sina uppgifter rättade av de skäl som anges, till exempel när det visas att de är felaktiga eller ofullständiga. Den registrerade ska även ha rätt att få sina uppgifter raderade, till exempel när behandlingen inte längre är nödvändig eller är olaglig.

53. Utövandet av dessa rättigheter ska inte vara alltför betungande för den registrerade.

k) Begränsningar av de registrerades rättigheter

54. Möjliga begränsningar av dessa rättigheter kan föreligga för att undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden, undvika menlig inverkan på förebyggande, förhindrande, utredning, upptäckt eller lagföring av brott eller verkställighet av straffrättsliga påföljder, skydd för allmän eller nationell säkerhet eller skydd för andra personers rättigheter och friheter, så länge en sådan partiell eller fullständig begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen. Sådana begränsningar bör även beaktas och bedömas med hänsyn till möjligheten att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning.

l) Begränsningar av vidare överföring av personuppgifter (artikel 35, skälen 64–65)

55. Den skyddsnivå som föreskrivs i unionen för fysiska personer vars uppgifter överförs får inte undergrävas genom vidare överföring av personuppgifter från den ursprungliga mottagaren till ett annat tredjeland eller en annan internationell organisation. Därför ska sådana vidare överföringar endast vara tillåtna om den skyddsnivå som föreskrivs enligt unionsrätten vidmakthålls[50]. I synnerhet ska den ytterligare mottagaren (dvs. mottagaren av den vidare överföringen) vara en behörig brottsbekämpande myndighet[51] och sådana vidare överföringar av

[49] Artikel 14 i direktivet om uppgiftsskydd vid brottsbekämpning.
[50] Se även yttrande 1/15.
[51] Se fotnot 33.

uppgifter får endast genomföras för begränsade och specifika ändamål och så länge som det finns en rättslig grund för denna behandling.

56. Det ska även beaktas om det finns en mekanism för att informera de relevanta medlemsstaternas behöriga myndigheter om sådan vidare överföring av uppgifter och genom vilken de kan godkänna överföringen. Ansvaret bör ligga på den ursprungliga mottagaren av de uppgifter som överförts från EU och denne ska kunna bevisa att medlemsstatens relevanta konkurrensmyndighet har godkänt den vidare överföringen[52] och att lämpliga säkerhetsåtgärder föreskrivs för vidare överföringar av uppgifter i avsaknad av ett beslut om adekvat skyddsnivå beträffande det tredjeland till vilket uppgifterna ska överföras vidare[53].

m) Ansvarsprincipen (artikel 4.4)

57. Den personuppgiftsansvarige ska ansvara för, och kunna visa efterlevnad av, de dataskyddsprinciper som återfinns i artikel 4 i direktivet om uppgiftsskydd vid brottsbekämpning.

[52] Det ska i detta sammanhang beaktas huruvida det föreligger en skyldighet eller ett åtagande att genomföra relevanta hanteringskoder som fastställts av den överförande medlemsstatens myndigheter.
[53] Ovannämnda krav påverkar inte de särskilda villkor för vidare överföringar till ett land med adekvat skyddsnivå som föreskrivs enligt direktivet om uppgiftsskydd vid brottsbekämpning (artikel 35.1 c och e).

B. Exempel på ytterligare principer som ska tillämpas för specifika typer av behandlingar

a) Särskilda kategorier av uppgifter (artikel 10 och skäl 37)

58. Specifika skyddsåtgärder bör vidtas när ”särskilda kategorier av uppgifter” är inblandade[54] för att hantera de särskilda risker som omfattas[55]. Dessa kategorier bör återspegla dem som anges i artikel 10 i direktivet om uppgiftsskydd vid brottsbekämpning. Behandling av särskilda kategorier av uppgifter ska därför vara föremål för särskilda säkerhetsåtgärder och endast vara tillåten när det är absolut nödvändigt under vissa omständigheter, exempelvis för att skydda intressen som är av grundläggande betydelse för en enskild person.

b) Automatiserat beslutsfattande och profilering (artikel 11 och skäl 38)

59. Beslut som enbart baseras på automatisk behandling (automatiserat individuellt beslutsfattande), inklusive profilering, som får negativa rättsliga följder för eller i betydande grad påverkar den registrerade, bör endast äga rum under vissa villkor som fastställs i tredjelandets rättsliga ramar[56].

60. Inom Europeiska unionens ramar omfattar sådana villkor bland annat skild information till den registrerade samt rätt till personlig kontakt med den personuppgiftsansvarige, särskilt för framförande av egna synpunkter, rätt att erhålla en förklaring för det beslut som fattats efter sådan bedömning och rätt att överklaga beslutet.

61. Lagstiftningen från tredjeland ska under alla omständigheter föreskriva nödvändiga säkerhetsåtgärder för den registrerades rättigheter och friheter. I detta avseende bör även förekomsten av en mekanism för att informera den relevanta medlemsstatens behöriga myndigheter om eventuell vidare behandling, exempelvis om de överförda uppgifterna används för omfattande profilering, beaktas.

c) Inbyggt dataskydd och dataskydd som standard (artikel 20)

62. Vid bedömningen huruvida adekvat skyddsnivå föreligger, ska det uppmärksammas om personuppgiftsansvariga är skyldiga att anta interna strategier och vidta åtgärder, som följer principerna om inbyggt dataskydd och dataskydd som standard med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, vidta lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering, vilka är utformade för ett effektivt genomförande av dataskyddsprinciper, såsom uppgiftsminimering, och för integrering av de nödvändiga skyddsåtgärderna i behandlingen.

[54] Dessa särskilda kategorier kallas även för ”känsliga uppgifter” i skäl 37 i direktivet om uppgiftsskydd vid brottsbekämpning.
[55] Sådana ytterligare säkerhetsåtgärder kan t.ex. utgöra särskilda säkerhetsåtgärder, begränsad åtkomst för personal, begränsningar av ytterligare behandling, automatiserat beslutsfattande, vidare delning och vidare överföringar.
[56] Yttrande 1/15, punkt 173.

C. Förfarande- och verkställandemekanismer

63. Även om de medel som tredjelandet använder för att säkerställa en adekvat skyddsnivå kan skilja sig från de som används inom EU[57], måste följande element finnas med för att ett system ska kunna räknas som förenligt med unionens:

a) Oberoende behörig tillsynsmyndighet (artikel 36.2 b och 36.3 och skäl 67)

64. Det ska finnas en eller flera oberoende tillsynsmyndigheter som har till uppgift att säkerställa och kontrollera att bestämmelserna om uppgiftsskydd och integritetsskydd efterlevs i tredjelandet. Tillsynsmyndigheten ska utföra sina uppgifter och utöva sina befogenheter på ett fullständigt oberoende och opartiskt sätt, och varken efterfråga eller ta emot några instruktioner. Tillsynsmyndigheten ska i detta sammanhang ha tillräckliga verkställande befogenheter för att på ett effektivt sätt säkerställa att rätten till uppgiftsskydd efterlevs och främja medvetenhet. Tillsynsmyndighetens personal och budget ska även tas under beaktande. Dessutom ska tillsynsmyndigheten ha möjlighet att på eget initiativ utföra utredningar. Den ska även ha i uppgift att bistå och ge råd till registrerade vid deras utövande av sina rättigheter (se även punkt c nedan). I beslut om adekvat skyddsnivå bör, i tillämpliga fall, denna tillsynsmyndighet eller dessa tillsynsmyndigheter identifieras tillsammans med de samarbetsmekanismer med medlemsstaternas tillsynsmyndigheter som finns för att kontrollera att bestämmelserna om dataskydd efterlevs.

b) Effektivt genomförande av dataskyddsbestämmelser

65. Systemet för skydd av personuppgifter i ett tredjeland ska säkerställa att personuppgiftsansvariga och de som behandlar personuppgifter på deras vägnar i hög grad är medvetna om de skyldigheter, uppgifter och ansvarsområden de omfattas av, samt att de registrerade känner till sina rättigheter och de medel de har för att utöva dem. Tillgång till effektiva och avskräckande sanktioner kan spela en viktig roll för att säkerställa respekten för bestämmelserna, vilket även gäller system för direktkontroll från myndigheters, revisorers eller oberoende dataskyddstjänstemäns sida.

66. De rättsliga ramarna för skydd av personuppgifter i ett tredjeland ska ställa som krav att personuppgiftsansvariga eller de som behandlar personuppgifter på deras vägnar efterlever ramarna och att de ska kunna styrka denna efterlevnad, i synnerhet för den behöriga tillsynsmyndigheten. Sådana åtgärder bör omfatta förande av register eller loggfiler för personuppgiftsbehandling som sparas under en lämplig tidsperiod. Till exempel kan de även omfatta konsekvensbedömningar avseende dataskydd, utnämning av ett dataskyddsombud eller inbyggt dataskydd och dataskydd som standard.

c) Systemet för skydd av personuppgifter ska underlätta utövandet av registrerades rättigheter (artiklarna 12, 17 och 46 i direktivet om uppgiftsskydd vid brottsbekämpning)

67. De rättsliga ramarna för skydd av personuppgifter i ett tredjeland bör ålägga personuppgiftsansvariga att underlätta utövandet av sådana rättigheter från registrerade till vilka hänvisas i avsnitt A j) ovan och föreskriva att dess tillsynsmyndighet på begäran ska informera registrerade om utövandet av deras rättigheter[58].

[57] Schrems I, punkt 74.
[58] Registrerades rättigheter kan utövas antingen direkt eller indirekt.

d) Systemet för skydd av personuppgifter ska tillhandahålla lämpliga prövningsmekanismer

68. Även om det för närvarande inte finns någon rättspraxis som rör frågan huruvida ett tredjelands rättssystem har en adekvat skyddsnivå enligt direktivet om uppgiftsskydd vid brottsbekämpning, har EU-domstolen tolkat den grundläggande rätten till effektivt rättsligt skydd i artikel 47 i stadgan. Enligt artikel 47 första stycket i stadgan krävs det att var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts har rätt till ett effektivt rättsmedel inför en domstol[59], med beaktande av de villkor som föreskrivs i denna artikel.

69. Enligt EU-domstolens fasta rättspraxis är själva möjligheten till effektiv domstolsprövning i syfte att säkerställa iakttagandet av unionsrätten en grundförutsättning för en rättsstat. En lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera personuppgifter som rör dem, respekterar inte det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, vilken är stadfäst i artikel 47 i stadgan[60].

70. Den enskilde ska kunna vidta rättsliga åtgärder för att hävda sina rättigheter på ett snabbt och effektivt sätt, och utan orimliga kostnader, liksom för att säkerställa att bestämmelserna efterlevs.

71. För att detta ska bli möjligt måste det finnas kontrollmekanismer som tillåter oberoende utredning av klagomål och gör det möjligt att i praktiken upptäcka och bestraffa eventuella överträdelser av rätten till uppgiftsskydd och respekt för privatlivet.

72. Om bestämmelserna inte efterlevs ska registrerade vars personuppgifter överförs till tredjelandet likaså tillförsäkras effektiv administrativ och rättslig prövning i tredjelandet, däribland för ersättning för skador som orsakats av den olagliga behandlingen av hans eller hennes personuppgifter. Detta är en nyckelfråga som kräver ett system med oberoende skiljedom så att ersättningar kan betalas ut och sanktioner utkrävas när detta är motiverat.

[59] EU-domstolen anser att ett effektivt rättsligt skydd inte enbart kan säkerställas genom domstol, utan även genom ett organ som ger garantier som är väsentligen likvärdiga med dem som krävs enligt artikel 47 i stadgan (se Schrems II, punkt 197). Detta kan särskilt vara relevant när det gäller internationella organisationer.
[60] Schrems II, punkterna 187 och 194 och där angiven rättspraxis.