

# Rekommendationer



## **Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder**

**Antagna den 10 november 2020**

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

## Innehållsförteckning

1. INLEDNING .....	4
2. INGREPP I DE GRUNDLÄGGANDE RÄTTIGHETERNA.....	6
3. DE EUROPEISKA NÖDVÄNDIGA GARANTIerna .....	8
Garanti A – Uppgifter bör behandlas utifrån tydliga, precisa och tillgängliga bestämmelser.....	8
Garanti B – Nödvändighet och proportionalitet ska säkerställas för legitima mål .....	10
Garanti C – En oberoende tillsynsmekanism bör finnas .....	12
Garanti D – Enskilda personer ska ha tillgång till effektiva rättsmedel .....	13
4. AVSLUTANDE ANMÄRKNINGAR .....	15

## Europeiska dataskyddsstyrelsen har antagit dessa rekommendationer

med beaktande av artikel 70.1 e i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan kallad *den allmänna dataskyddsförordningen*)<sup>1</sup>,

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018<sup>2</sup>,

med beaktande av artiklarna 12 och 22 i arbetsordningen, och

med beaktande av artikel 29-gruppens arbetsdokument *Working Document on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)*, arbetsgrupp 237 (ej översatt till svenska).

### HÄRIGENOM REKOMMENDERAS FÖLJANDE.

## 1. INLEDNING

1. De europeiska nödvändiga garantierna har fastställts av EU-dataskyddsmyndigheterna i artikel 29-gruppen på grundval av domen i målet Schrems I. Dessa garantier måste respekteras för att se till att ingrepp i rättigheterna till privatliv och skydd av personuppgifter, som görs genom övervakningsåtgärder vid överföring av personuppgifter, inte går utöver vad som är nödvändigt och proportionellt i ett demokratiskt samhälle.

2. Europeiska dataskyddsstyrelsen vill understryka att de europeiska nödvändiga garantierna är baserade på rättspraxis från Europeiska unionens domstol (nedan kallad *domstolen*) som rör artiklarna 7, 8, 47 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och, i förekommande fall, på rättspraxis från Europeiska domstolen för de mänskliga rättigheterna (nedan kallad *Europadomstolen*) som rör artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (nedan kallad *Europakonventionen*) som behandlar övervakningsfrågor i stater som är parter i Europakonventionen<sup>3</sup>.

---

<sup>1</sup> Detta dokument berör inte fall av överföringar eller vidarebefordran som omfattas av direktiv (EU) 2016/680.

<sup>2</sup> Hänvisningar till "medlemsstater" som görs i hela detta dokument ska förstås som hänvisningar till "EES-medlemsstater".

<sup>3</sup> I dessa rekommendationer har termen "grundläggande rättigheter" samma betydelse som i stadgan. Den används dock också i betydelsen "mänskliga rättigheter" enligt Europakonventionen.

3. Syftet med att uppdatera detta dokument är att vidareutveckla de europeiska nödvändiga garantierna, som ursprungligen utarbetades som svar på domen i målet Schrems I<sup>4</sup>, genom att återspegla de klagöranden som gjorts av domstolen (och av Europadomstolen) sedan dokumentet först offentliggjordes, särskilt den prejudikatbildande Schrems II-domen<sup>5</sup>.

4. I Schrems II-domen konstaterade domstolen att det vid prövningen av kommissionens beslut 2010/87/EU om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland, mot bakgrund av artiklarna 7, 8 och 47 i stadgan, inte hade framkommit någon omständighet som påverkade beslutets giltighet, men att beslutet om skölden för skydd av privatlivet var ogiltigt. EU-domstolen ansåg att beslutet om skölden för skydd av privatlivet stred mot artikel 45.1 i den allmänna dataskyddsförordningen, mot bakgrund av artiklarna 7, 8 och 47 i stadgan. Domen kan därmed tjäna som ett exempel på övervakningsåtgärder i tredjeland (i detta fall Förenta staterna med sektion 702 i *Foreign Intelligence Surveillance Act* och dekret 12333) som varken är tillräckligt begränsade eller omfattas av möjligheter till effektiv rättslig prövning som står öppna för registrerade som vill hävda sina rättigheter, vilket krävs enligt EU-rätten för att anse att skyddsnivån i ett tredjeland ”i huvudsak motsvarar” den som säkerställs i Europeiska unionen i den mening som avses i artikel 45.1 i den allmänna dataskyddsförordningen.

5. Skälen till ogiltigförklarandet av skölden för skydd av privatlivet har också konsekvenser för andra överföringsverktyg<sup>6</sup>. Även om domstolen tolkade artikel 46.1 i den allmänna dataskyddsförordningen inom ramen för standardavtalsklausulernas giltighet är denna tolkning tillämplig på varje överföring till ett tredjeland som görs med hjälp av något av de verktyg som avses i artikel 46 i den allmänna dataskyddsförordningen<sup>7</sup>.

6. I slutändan är det upp till domstolen att avgöra huruvida ingrepp i en grundläggande rättighet kan vara motiverade. I avsaknad av en sådan dom och vid tillämpning av gällande rättspraxis är dataskyddsmyndigheterna dock skyldiga att bedöma enskilda fall, antingen på eget initiativ eller till följd av ett klagomål, och att antingen hänskjuta fallet till en nationell domstol om de misstänker att överföringen inte uppfyller artikel 45 där det finns ett beslut om adekvat skyddsnivå, eller att avbryta eller förbjuda överföringen om de konstaterar att artikel 46 i den allmänna dataskyddsförordningen inte kan uppfyllas och att det skydd för överförda uppgifter som krävs enligt EU-rätten inte kan säkerställas på andra sätt.

7. Syftet med de uppdaterade europeiska nödvändiga garantierna är att presentera delar som ska bedömas för att avgöra om övervakningsåtgärder, som gör det möjligt för offentliga myndigheter (dvs. nationella säkerhetsmyndigheter eller brottsbekämpande myndigheter) i ett tredjeland att få tillgång till personuppgifter, kan betraktas som motiverade ingrepp.

---

<sup>4</sup> EU-domstolens dom av den 6 oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, EU:C:2015:650 (nedan kallad *Schrems I*).

<sup>5</sup> EU-domstolens dom av den 16 juli 2020, Data Protection Commissioner/Facebook Ireland Limited och Maximilian Schrems, C-311/18, ECLI:EU:C:2020:559 (nedan kallad *Schrems II*).

<sup>6</sup> Se § 105 i *Schrems II*.

<sup>7</sup> Se § 92 i *Schrems II*.

8. De europeiska nödvändiga garantierna ingår i den bedömning som ska utföras för att avgöra om ett tredjeland ger en skyddsnivå som i huvudsak motsvarar den som säkerställs inom EU, men de syftar inte till att i sig fastställa alla delar som krävs för att ett tredjeland ska anses ge en sådan skyddsnivå i enlighet med artikel 45 i den allmänna dataskyddsförordningen. De syftar inte heller till att i sig fastställa alla delar som bör beaktas vid bedömningen av huruvida ett tredjelands rättsliga regelverk hindrar uppgiftsutförare och uppgiftsinförare att säkerställa lämpliga skyddsåtgärder i enlighet med artikel 46 i den allmänna dataskyddsförordningen.

9. De delar som presenteras i detta dokument bör därför betraktas som nödvändiga garantier som ska finnas i tredjelandet vid bedömningen av ett ingrepp, som följer av övervakningsåtgärder i ett tredjeland, i förhållande till rättigheterna till privatliv och skydd av personuppgifter, snarare än en förteckning över delar som visar att ett tredjelands rättsliga regelverk som helhet erbjuder en i huvudsak motsvarande skyddsnivå.

10. Enligt artikel 6.3 i fördraget om Europeiska unionen ska de grundläggande rättigheterna, såsom de garanteras i Europakonventionen, ingå i EU-rätten som allmänna principer. EU-domstolen påminner dock i sin rättspraxis om att Europakonventionen inte utgör något rättsligt instrument som formellt införlivats med EU-rätten så länge som inte Europeiska unionen har anslutit sig till konventionen<sup>8</sup>. Den skyddsnivå för grundläggande rättigheter som krävs enligt artikel 46.1 i den allmänna dataskyddsförordningen ska därför fastställas på grundval av bestämmelserna i den förordningen, mot bakgrund av de grundläggande rättigheter som erkänns i stadgan. Oavsett detta och enligt artikel 52.3 i stadgan ska de rättigheter som omfattas av stadgan och som motsvarar sådana som garanteras av Europakonventionen ha samma innebörd och räckvidd som i konventionen. Följaktligen, såsom domstolen har poängterat, ska rättspraxis från Europadomstolen som rör rättigheter som även avses i stadgan beaktas, som en lägsta skyddsnivå vid tolkningen av motsvarande rättigheter i stadgan<sup>9</sup>. I sista meningen i artikel 52.3 i stadgan anges dock att denna bestämmelse inte hindrar unionsrätten från att tillförsäkra ett mer långtgående skydd.

11. Av denna anledning kommer innehållet i de nödvändiga garantierna fortsättningsvis att vara delvis baserade på rättspraxis från Europadomstolen, i den utsträckning som stadgan, enligt domstolens tolkning, inte medför en högre skyddsnivå som föreskriver andra krav än de i rättspraxis från Europadomstolen.

12. Detta dokument innehåller en beskrivning av bakgrunden och närmare information om de fyra europeiska nödvändiga garantierna.

## 2. INGREPP I DE GRUNDLÄGGANDE RÄTTIGHETERNA

13. De grundläggande rättigheterna respekt för privatlivet och familjelivet, inklusive kommunikationer, och skydd av personuppgifter, fastställs i artiklarna 7 och 8 i stadgan och gäller för alla. I artikel 8 anges dessutom krav på att uppgifter ska behandlas lagenligt, rätten att få tillgång till och rättelse av uppgifter erkänns och det föreskrivs att en oberoende myndighet ska kontrollera att dessa regler efterlevs.

---

<sup>8</sup> Se § 98 i Schrems II.

<sup>9</sup> Se § 124 i förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.* (nedan kallade *La Quadrature du Net m.fl.*).

14. Det har konstaterats att "åtgärden att låta överföra personuppgifter från en medlemsstat till ett tredjeland i sig utgör en behandling av personuppgifter"<sup>10</sup>. Artiklarna 7 och 8 i stadgan är därför tillämpliga på denna åtgärd och skyddet omfattar de uppgifter som överförs, vilket innebär att det ska säkerställas att personer vars personuppgifter överförs till ett tredjeland åtnjuter en skyddsnivå som är väsentligen likvärdig med den som garanteras inom Europeiska unionen<sup>11</sup>.

15. Enligt domstolen påverkar behandlingar av en fysisk persons personuppgifter också denna persons grundläggande rätt till respekt för privatlivet, vilken garanteras i artikel 7 i stadgan. Nämnda behandlingar av personuppgifter omfattas även av artikel 8 i stadgan och de måste därför uppfylla de krav på skydd av uppgifter som följer av den artikeln<sup>12</sup>.

16. Vad gäller möjliga ingrepp i grundläggande rättigheter enligt EU-rätten innebär detta att skyldigheten för leverantörer av elektroniska kommunikationstjänster att lagra trafikuppgifter för att de behöriga nationella myndigheterna i tillämpliga fall ska kunna få tillgång till dessa, ger upphov till frågor om förenligheten med artiklarna 7 och 8 i stadgan<sup>13</sup>. Samma sak gäller även för andra typer av uppgiftsbehandlingar, till exempel överföring av uppgifter till andra personer än användarna eller tillgång till uppgifter i syfte att använda dem<sup>14</sup>, vilket därmed innebär ett ingrepp i dessa grundläggande rättigheter. Dessutom utgör offentliga myndigheters tillgång till uppgifterna ett ytterligare ingrepp, enligt fast rättspraxis<sup>15</sup>.

17. För att ett ingrepp ska konstateras har det "föga betydelse huruvida de uppgifter som avser privatlivet är av känslig art eller huruvida de berörda har fått utstå eventuella olägenheter på grund av ingreppet eller inte"<sup>16</sup>. EU-domstolen framhöll även att det inte är relevant om de lagrade uppgifterna därefter används eller inte<sup>17</sup>.

18. Artiklarna 7 och 8 i stadgan är emellertid inte absoluta rättigheter, utan måste förstås utifrån sin funktion i samhället<sup>18</sup>.

19. Stadgan omfattar en nödvändighets- och proportionalitetskontroll för att utforma begränsningar efter de rättigheter som den skyddar. I artikel 52.1 i stadgan anges omfattningen av möjliga begränsningar av artiklarna 7 och 8 enligt följande: "Varje begränsning i utövandet av de rättigheter och friheter som erkänns i denna stadga ska vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter."

---

<sup>10</sup> EU-domstolens dom, Schrems II, § 83.

<sup>11</sup> EU-domstolens dom, Schrems II, § 96.

<sup>12</sup> EU-domstolen, Schrems II, §§ 170–171.

<sup>13</sup> EU-domstolen, *Privacy International*, C-623/17 (nedan kallad *Privacy International*), § 60.

<sup>14</sup> EU-domstolen, *Privacy International*, § 61.

<sup>15</sup> Europadomstolen, *Leander*, § 48; Europadomstolen, *Rotaru*, § 46; EU-domstolen, *Digital Rights Ireland*, § 35.

<sup>16</sup> EU-domstolen, Schrems II, § 171, och däri angiven rättspraxis.

<sup>17</sup> EU-domstolen, Schrems II, § 171, och däri angiven rättspraxis.

<sup>18</sup> EU-domstolen, *Privacy International*, § 63.

20. EU-domstolen bekräftade att EU-lagstiftning som omfattar ingrepp i de grundläggande rättigheter som garanteras genom artiklarna 7 och 8 i stadgan måste innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt fastställer minimikrav, så att de personer vars personuppgifter påverkas har tillräckliga garantier för att uppgifterna effektivt skyddas mot risken för missbruk, särskilt om personuppgifterna är föremål för automatisk behandling och om det finns en betydande risk för olaglig tillgång till dessa uppgifter<sup>19</sup>.

21. Enligt domstolen ska undantag från och begränsningar av rättigheten till dataskydd inskränkas till vad som är absolut nödvändigt. Dessutom ska mål av allmänt intresse förenas med de grundläggande rättigheter som påverkas av åtgärden, genom att korrekt balansera sådana mål mot rättigheterna i fråga<sup>20</sup>.

22. Följaktligen får offentliga myndigheters tillgång, lagring och vidareanvändning av personuppgifter inom ramen för övervakningsåtgärder inte överskrida gränserna för vad som är absolut nödvändigt, vilket bedöms mot bakgrund av stadgan, annars kan det inte anses motiverat i ett demokratiskt samhälle<sup>21</sup>.

23. Syftet med de fyra europeiska nödvändiga garantierna, vilka beskrivs i nästa kapitel, är att ytterligare specificera hur man bedömer nivån av ingrepp i de grundläggande rättigheterna till privatliv och dataskydd i samband med övervakningsåtgärder som vidtas av offentliga myndigheter i ett tredjeland vid behandling av personuppgifter, samt vilka rättsliga krav som följligen ska vara tillämpliga för att avgöra om dessa ingrepp är godtagbara enligt stadgan.

### 3. DE EUROPEISKA NÖDVÄNDIGA GARANTIerna

24. Efter en analys av rättspraxis anser Europeiska dataskyddsstyrelsen att de tillämpliga rättsliga krav som kan motivera begränsningar av rättigheterna till dataskydd och privatliv enligt stadgan kan sammanfattas i följande fyra europeiska nödvändiga garantier:

- A. Uppgifter bör behandlas utifrån tydliga, precisa och tillgängliga bestämmelser.
- B. Nödvändighet och proportionalitet ska säkerställas för legitima mål.
- C. En oberoende tillsynsmekanism bör finnas.
- D. Enskilda personer ska ha tillgång till effektiva rättsmedel.

25. Garantierna är baserade på de grundläggande rättigheterna till privatliv och dataskydd som gäller för alla, oavsett nationalitet.

#### Garanti A – Uppgifter bör behandlas utifrån tydliga, precisa och tillgängliga bestämmelser

26. 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 grund", vilket domstolen framhöll i Schrems II-domen<sup>22</sup>. I artikel 52.1 i stadgan anges dessutom att varje begränsning

---

<sup>19</sup> EU-domstolen, Privacy International, § 68, samt däri angiven rättspraxis.

<sup>20</sup> EU-domstolen, Privacy International, § 68, samt däri angiven rättspraxis.

<sup>21</sup> EU-domstolen, Privacy International, § 81.

<sup>22</sup> Se § 173 i Schrems II.

av utövandet av de rättigheter och friheter som erkänns i stadgan inom EU ska vara föreskriven i lag. Ett motiverat ingrepp måste därmed vara i överensstämmelse med lagstiftning.

27. Denna rättsliga grund bör innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt fastställer minimikrav<sup>23</sup>. Domstolen framhöll även att lagstiftning ska vara rättsligt bindande enligt nationell lagstiftning<sup>24</sup>. I denna fråga klargjorde EU-domstolen att bedömningen av den tillämpliga lagstiftningen i tredjelandet bör inriktas på huruvida den kan åberopas och anföras av enskilda personer vid en domstol<sup>25</sup>. Domstolen anger därför att de registrerades rättigheter ska kunna göras gällande. Om enskilda personer inte har tillgång till verkställbara rättigheter mot offentliga myndigheter kan den skyddsnivå som ges inte anses vara väsentligen likvärdig med den som följer av stadgan, vilket strider mot kraven enligt artikel 45.2 a i den allmänna dataskyddsförordningen<sup>26</sup>.

28. Dessutom framhöll domstolen att den tillämpliga lagstiftningen ska ange under vilka omständigheter och på vilka villkor en åtgärd som gör det möjligt att behandla sådana uppgifter får antas<sup>27</sup> (se garanti B nedan om förhållandet mellan dessa krav och principerna om nödvändighet och proportionalitet).

29. EU-domstolen har dessutom angett att ”kravet på att samtliga begränsningar i utövandet av grundläggande rättigheter ska vara föreskrivna i lag, innebär att den rättsliga grund som gör ingreppet i rättigheterna möjligt i sig ska definiera räckvidden av begränsningen i utövandet av den aktuella rättigheten”<sup>28</sup>.

30. Slutligen anser Europadomstolen att det inte finns några skäl att tillämpa andra principer för tillgänglighet och tydlighet vad gäller bestämmelser som reglerar avlyssning av enskild kommunikation och mer allmänna övervakningsprogram<sup>29</sup>. Europadomstolen har även klargjort att den rättsliga grunden åtminstone bör omfatta en definition av de kategorier av människor som kan komma att övervakas, en tidsgräns för åtgärden, det förfarande som ska följas vid undersökning, användning och lagring av de uppgifter som erhålls, samt de försiktighetsåtgärder som ska vidtas när uppgifterna meddelas andra parter<sup>30</sup>.

31. Avslutningsvis ska ingreppets verkan vara förutsägbar, så att enskilda ges tillräckligt och effektivt skydd mot godtyckliga ingrepp och risken för missbruk. Uppgifter ska följaktligen behandlas utifrån en rättslig grund som är tydlig, precis och även tillgänglig (dvs. offentlig)<sup>31</sup>. I denna fråga framhöll Europadomstolen i målet Sacharov att ”hänvisningen till ’förutsägbarhet’ när det gäller

---

<sup>23</sup> Se § 175 och § 180 i Schrems II, samt yttrande 1/15 (Avtal om passageraruppgifter mellan EU och Kanada) av den 26 juli 2017, § 139, samt däri angiven rättspraxis.

<sup>24</sup> Se § 68 i Privacy International – Det bör förtydligas att domstolen använder ordet ”réglementation” i den franska versionen av domen, vilket omfattar mer än endast parlamentsakter.

<sup>25</sup> Se § 181 i Schrems II, där EU-domstolen hänvisar till Förenta staternas *Presidential Policy Directive 28*.

<sup>26</sup> Se § 181 i Schrems II.

<sup>27</sup> Se § 68 i Privacy International, avseende medlemsstatslagstiftning.

<sup>28</sup> Se Schrems II, § 175 och däri angiven rättspraxis, samt Privacy International, § 65.

<sup>29</sup> Europadomstolen, Liberty, § 63.

<sup>30</sup> Europadomstolen, Weber and Saravia, § 95.

<sup>31</sup> Europadomstolen, Malone, §§ 65 och 66.



kommunikationsavlyssning inte kan vara densamma som inom många andra områden". Förutsägbarheten i det särskilda sammanhanget med hemliga övervakningsåtgärder som t.ex. kommunikationsavlyssning, kan inte betyda att en enskild person ska kunna förutse när myndigheterna ska komma att avlyssna dennes kommunikation och anpassa denna därefter. I synnerhet när den verkställande makten utövas i hemlighet är risken för godtycke emellertid uppenbar. Därför är det ytterst viktigt att ha klara och detaljerade regler beträffande avlyssning av telefonsamtal, i synnerhet [sic] eftersom tillgänglig teknik för detta ständigt blir mer och mer sofistikerad. Den inhemska lagen måste vara tillräckligt tydlig, så att medborgarna får en tillfredsställande anvisning om de omständigheter som måste råda för att offentliga myndigheter ska ha rätt att tillgripa sådana åtgärder, och villkoren för detta"<sup>32</sup>.

## Garanti B – Nödvändighet och proportionalitet ska säkerställas för legitima mål

32. Enligt första meningen i artikel 52.1 i stadgan ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan vara förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Av artikel 52.1 andra meningen i stadgan följer vidare att begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter<sup>33</sup>.

33. Vad gäller **proportionalitetsprincipen** ansåg domstolen, avseende medlemsstatslagstiftning, att frågan om huruvida en begränsning i rättigheterna till privatliv och dataskydd är motiverad måste bedömas dels genom att mäta **allvaret hos ingreppet** som begränsningen medför<sup>34</sup>, dels genom att kontrollera att **betydelsen av målet av allmänt intresse** som eftersträvas med begränsningen står i proportion till allvaret<sup>35</sup>.

34. I La Quadrature du Net m.fl. kan det noteras att EU-domstolen slog fast att betydelsen av målet att skydda den nationella säkerheten – när det gäller lagstiftningen i en medlemsstat och inte i ett tredjeland – kan motivera åtgärder som innebär allvarligare ingrepp i de grundläggande rättigheterna än vad som kan motiveras av andra mål, till exempel brottsbekämpning. Domstolen fann dock att detta gäller så länge det finns tillräckligt hållbara grunder för att anse att den berörda staten står inför ett allvarligt hot mot den nationella säkerheten som har visats vara verkligt och aktuellt eller förutsebart, samt under förutsättning att de andra kraven i artikel 52.1 i stadgan uppfylls<sup>36</sup>.

---

<sup>32</sup> Europadomstolen, Sacharov, § 229.

<sup>33</sup> Schrems II, § 174.

<sup>34</sup> I denna fråga noterade domstolen bland annat att ingrepp i form av insamling av personuppgifter i realtid som gör det möjligt att lokalisera terminalutrustning förefaller särskilt allvarliga, eftersom sådana uppgifter gör att de behöriga nationella myndigheterna exakt och permanent kan spåra mobiltelefonanvändares rörelser (La Quadrature du Net m.fl., § 187, och däri angiven rättspraxis).

<sup>35</sup> La Quadrature du Net m.fl., § 131.

<sup>36</sup> §§ 136 och 137. Se även Privacy International, där domstolen angav att sådana hot genom deras art och särskilda allvar kan särskiljas från den allmänna risken för spänningar och oroligheter, också allvarliga sådana, som påverkar den allmänna säkerheten. § 75. Exempelvis noterade domstolen i La Quadrature du Net m.fl. att automatisk analys av trafik- och lokaliseringssuppgifter som generellt och odifferentierat omfattar uppgifter för personer som använder elektroniska kommunikationssystem, utgör ett ingrepp som är så pass allvarligt att denna åtgärd endast kan uppfylla proportionalitetskravet i situationer då den berörda medlemsstaten står inför ett allvarligt hot mot

35. Enligt fast rättspraxis kan kravet på proportionalitet endast uppfyllas om undantag från och inskränkningar i skyddet av personuppgifter begränsas till vad som är absolut nödvändigt<sup>37</sup>. För att uppfylla detta krav måste den aktuella lagstiftningen, utöver att innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden, även innehålla bestämmelser som fastställer 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."<sup>38</sup>

36. EU-domstolen framhöll i Schrems II att lagstiftning i ett tredjeland som inte omfattar några begränsningar av behörigheten att genomföra övervakningsprogram för att inhämta utländska underrättelseuppgifter, inte kan säkerställa en skyddsnivå som är väsentligen likvärdig med den som garanteras i stadgan. Enligt denna 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<sup>39</sup>.

37. Vad gäller **nödvändighetsprincipen** har EU-domstolen klargjort att en lagstiftning inte är förenlig med denna princip när den "generellt tillåter lagring av samtliga personuppgifter om alla personer vilkas uppgifter har överförts från unionen [...], utan att det görs några åtskillnader, begränsningar eller undantag med beaktande av det eftersträlvade syftet och utan att det föreskrivs något objektiva kriterium som gör det möjligt att avgränsa myndigheternas åtkomst till uppgifterna och att avgränsa deras senare användning till bestämda, strängt begränsade syften som kan motivera det ingrepp som såväl åtkomst som användning av uppgifterna innebär"<sup>40</sup>. I synnerhet måste en lagstiftning som tillåter myndigheterna generell åtkomst till innehållet i elektroniska kommunikationer anses kränka det väsentliga innehållet i den grundläggande rätten till respekt för privatlivet, som garanteras i artikel 7 i stadgan<sup>41</sup>.

38. I *La Quadrature du Net* m.fl. fann domstolen även, dock denna gång vid bedömning av lagstiftningen i en medlemsstat och inte i ett tredjeland, att lagstiftning som kräver lagring av personuppgifter alltid ska uppfylla objektiva kriterier som upprättar en koppling mellan de lagrade uppgifterna och det

---

den nationella säkerheten som har visats vara verkligt och aktuellt eller förutsebart, samt, bland andra villkor, under förutsättning att uppgifterna endast lagras så länge som är absolut nödvändigt (§§ 174–177).

<sup>37</sup> Schrems II, § 176, inklusive däri angiven rättspraxis.

<sup>38</sup> Schrems II, § 175.

<sup>39</sup> Schrems II, § 180.

<sup>40</sup> Schrems I, § 93, med ytterligare hänvisningar. Se *Privacy International*, § 71 och däri angiven rättspraxis, men denna gång med fokus på lagstiftningen i en medlemsstat och inte i ett tredjeland. I det fallet påpekade domstolen att kravet i en medlemsstats lagstiftning att leverantörer av elektroniska kommunikationstjänster måste lämna ut trafik- och lokaliseringssuppgifter till säkerhets- och underrättelseorgan genom generell och odifferentierad överföring överskrider gränserna för vad som är absolut nödvändigt och inte kan anses vara motiverat i ett demokratiskt samhälle, såsom fastställs i direktivet om integritet och elektronisk kommunikation, jämfört med stadgan (§ 81).

<sup>41</sup> Schrems I, § 94.

eftersträvade syftet<sup>42</sup>. I samma sammanhang fann domstolen i Privacy International att lagstiftaren måste använda sig av objektiva kriterier för att fastställa under vilka omständigheter och på vilka villkor de behöriga nationella myndigheterna ska ges tillgång till uppgifterna i fråga<sup>43</sup>.

## Garanti C – En oberoende tillsynsmekanism bör finnas

39. Europeiska dataskyddsstyrelsen framhåller att ett ingrepp sker både när uppgifterna samlas in och när en offentlig myndighet får tillgång till dem för vidare behandling. Europadomstolen har vid flera tillfällen angett att alla ingrepp i rättigheten till privatliv och dataskydd bör vara föremål för ett effektivt, oberoende och opartiskt tillsynssystem som ska genomföras av antingen en domare eller ett annat oberoende organ<sup>44</sup> (t.ex. en förvaltningsmyndighet eller en parlamentsinstans). Oberoende tillsyn över genomförandet av övervakningsåtgärder beaktades också av EU-domstolen i Schrems II-domen<sup>45</sup>.

40. Europadomstolen anger att även om (rättsligt) förhandsgodkännande av övervakningsåtgärder är en viktig skyddsåtgärd mot godtycke måste hänsyn också tas till det faktiska genomförandet av avlyssningssystemet, inklusive kontroller av och motvikter till maktutövningen, och till förekomst eller avsaknad av faktiskt missbruk<sup>46</sup>. I Schrems II beaktade EU-domstolen även räckvidden av den kontroll som utfördes av tillsynsmekanismen, vilken inte omfattade individuella övervakningsåtgärder<sup>47</sup>.

41. Vad gäller medlemsstaternas lagstiftning identifierade domstolen ett antal åtgärder som endast uppfyller EU-lagstiftningen om de är underkastade en effektiv kontroll av en domstol eller oberoende förvaltningsmyndighet vars beslut är bindande. Syftet med denna kontroll är att bekräfta att en situation som motiverar åtgärden föreligger och att de villkor och skyddsåtgärder som måste fastställas iakttas<sup>48</sup>. För insamling av trafik- och lokaliseringssuppgifter i realtid bör kontrollen göra det möjligt att på förhand bekräfta bland annat om åtgärden är godkänd endast inom gränserna för vad som är strängt nödvändigt. I vederbörligen underbyggda brådskande fall får åtgärderna vidtas utan en sådan förhandskontroll, men domstolen kräver då fortfarande att den efterföljande kontrollen utförs inom en kort tidsperiod<sup>49</sup>.

---

<sup>42</sup> La Quadrature du Net m.fl., § 133. I detta sammanhang bekräftade domstolen att lagstiftningsåtgärder som föreskriver förebyggande åtgärder för generell och odifferentierad lagring av trafik- och lokaliseringssuppgifter hindras av direktivet om integritet och elektronisk kommunikation, tolkat mot bakgrund av stadgan. Däremot fastställde domstolen att lagstiftaren, i situationer då den nationella säkerheten står inför ett allvarligt hot som har visats vara verkligt och aktuellt eller förutsebart, får medge användning av en bestämmelse som kräver att leverantörer av elektroniska kommunikationstjänster generellt och odifferentierat lagrar trafik- och lokaliseringssuppgifter, om detta krävs för att skydda den nationella säkerheten. En sådan åtgärd måste dock uppfylla särskilda villkor. I synnerhet får bestämmelsen endast gälla under en tidsperiod som är begränsad till vad som är absolut nödvändigt, vilken får förlängas om hotet kvarstår (§ 168).

<sup>43</sup> Privacy International, § 78 och däri angiven rättspraxis. Avseende en myndighets tillgång till personuppgifter enligt lagstiftningen i en medlemsstat fastställde domstolen i målet Privacy International att allmän tillgång till alla lagrade uppgifter inte kan anses vara begränsad till vad som är absolut nödvändigt, oavsett om det finns en koppling, åtminstone en indirekt sådan, till det eftersträvade syftet (§ 77–78).

<sup>44</sup> Europadomstolen, Klass, §§ 17 och 51.

<sup>45</sup> Schrems II, §§ 179 och 183.

<sup>46</sup> Europadomstolen, Big Brother Watch, överklagad, §§ 319–320.

<sup>47</sup> Schrems II, § 179.

<sup>48</sup> EU-domstolen, La Quadrature du Net m.fl., §§ 168 och 189.

<sup>49</sup> EU-domstolen, La Quadrature du Net m.fl., § 189.

42. När det gäller oberoendet hos tillsynsmekanismer i samband med övervakning kan domstolens iakttagelser om oberoendet hos ett organ inom ramen för prövning beaktas (se garanti D nedan). Dessutom kan ytterligare delar finnas i rättspraxis från Europadomstolen. Denna domstol har uttryckt sin preferens för en domare som tillsynsansvarig. Det är dock inte uteslutet att en annan myndighet kan vara ansvarig, "förutsatt att den myndigheten är tillräckligt självständig i förhållande till den verkställande makten"<sup>50</sup> och "gentemot de myndigheter som bedriver tillsynen, och har tillräckliga befogenheter och behörighet att utöva verksam och fortlöpande kontroll"<sup>51</sup>. Europadomstolen tillade att hänsyn måste tas till "utnämning av och rättstatus för tillsynsorganets personal"<sup>52</sup> när självständigheten bedöms. Detta omfattar "personer som var behöriga att inneha juridiska befattningar, antingen utsedda av parlamentet eller av premiärministern [...]. I motsats befanns en inrikesminister – som inte bara var politiskt utsedd och medlem av den verkställande makten, utan också direkt engagerad i förordnandet av särskilda övervakningsmedel – inte vara tillräckligt självständig"<sup>53</sup>. Europadomstolen noterar även att "det är avgörande att tillsynsorganet får tillgång till allt material av betydelse, också hemligstämplat sådant"<sup>54</sup>. Slutligen måste Europadomstolen också pröva "huruvida tillsynsorganets verksamhet är öppen för offentlig granskning"<sup>55</sup>.

### Garanti D – Enskilda personer ska ha tillgång till effektiva rättsmedel

43. Den sista europeiska nödvändiga garantin rör enskilda personers rätt till prövning. Enskilda ska ha ett effektivt rättsmedel för att tillgodose deras rättigheter när de anser att dessa åsidosatts eller har åsidosatts. EU-domstolen förklarade följande i Schrems I: "En lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera uppgifter som rör dem, respekterar inte det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, vilken är stadfäst i artikel 47 i stadgan. I artikel 47 första stycket i stadgan föreskrivs nämligen att var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts har rätt till ett effektivt rättsmedel inför en domstol, med beaktande av de villkor som föreskrivs i den artikeln."<sup>56</sup>

44. Vid en bedömning av en medlemsstats lagstiftning som tillåter insamling av trafik- och lokaliseringssuppgifter i realtid ansåg domstolen att det är nödvändigt att informera de berörda personerna om detta för att de ska kunna utöva sina rättigheter enligt artiklarna 7 och 8 i stadgan att begära tillgång till, samt eventuellt rättelse och radering av, egna personuppgifter som har varit föremål för dessa åtgärder och att, i enlighet med artikel 47 första meningen i stadgan, utnyttja ett effektivt rättsmedel inför en domstol<sup>57</sup>. Dock erkänns även att de personer vars uppgifter har samlats in eller analyserats ska informeras om detta endast i den utsträckning och så snart som denna information inte längre äventyrar den verksamhet som myndigheterna är ansvariga för<sup>58</sup>.

---

<sup>50</sup> Europadomstolen, Sacharov, § 258, Iordachi and Others v. Moldova, §§ 40 och 51, samt Dumitru Popescu v. Romania, §§ 70–73.

<sup>51</sup> Europadomstolen, Klass, § 56, samt Big Brother Watch, överklagad, § 318.

<sup>52</sup> Europadomstolen, Sacharov, § 278.

<sup>53</sup> Europadomstolen, Sacharov, § 278.

<sup>54</sup> Europadomstolen, Sacharov, § 281.

<sup>55</sup> Europadomstolen, Sacharov, § 283.

<sup>56</sup> EU-domstolen, Schrems I, § 95.

<sup>57</sup> Se § 190 i La Quadrature du Net m.fl., samt EU-domstolens yttrande 1/15, § 220.

<sup>58</sup> Se §191 i La Quadrature du Net m.fl.

45. Även för Europadomstolen är frågan om effektivt rättsmedel oupplösligt knuten till att enskilda informeras om en övervakningsåtgärd när övervakningen är över. Domstolen konstaterade särskilt att det i princip finns "små möjligheter för den berörda personen att vända sig till domstol, såvida inte denne blir informerad om de åtgärder som vidtagits utan hans/hennes vetskap och på så sätt kan bestrida lagligheten för dessa retroaktivt [...] eller, som alternativ, såvida inte någon person som misstänker att hans/hennes kommunikation håller på att eller har avlyssnats kan vända sig till domstol så att domstolarnas domsrätt inte är avhängig något meddelande till den avlyssnade personen om att det har förekommit avlyssning av hans/hennes kommunikation"<sup>59</sup>. Europadomstolen medgav därmed att ett meddelande i vissa fall kan saknas, men att ett effektivt rättsmedel måste tillhandahållas trots detta. I sådana fall har domstolen gjort tydligt, till exempel i målet Kennedy, att en domstol erbjuder tillräckliga möjligheter till prövning om den uppfyller en serie kriterier, dvs. om det finns ett oberoende och opartiskt organ som har antagit sin egen arbetsordning och består av medlemmar som har eller har haft ett högt domarämbete eller som är erfarna jurister, samt om det inte finns någon bevisbörla som måste uppfyllas för att lämna in en ansökan hos detta organ<sup>60</sup>. När domstolen undersöker klagomål från enskilda bör den få tillgång till all information av betydelse<sup>61</sup>, också hemligstämplad sådan. Slutligen bör den ha befogenheter att åtgärda bristande efterlevnad<sup>62</sup>.

46. I artikel 47 i stadgan används i den engelska versionen ordet "tribunal", men i de andra språkversionerna används främst ord som motsvarar "court" ("domstol" i den svenska versionen)<sup>63</sup>. Enligt Europakonventionen ska medlemsstaterna dock endast säkerställa att var och en, vars fri- och rättigheter kränkts, ska ha tillgång till ett effektivt rättsmedel inför en "nationell myndighet"<sup>64</sup>, vilket inte nödvändigtvis behöver vara en rättslig myndighet<sup>65</sup>.

47. EU-domstolen har bekräftat, i samband med Schrems II-domen vid bedömningen av huruvida ett tredjeland säkerställer en adekvat skydds nivå, att "enskilda ska ha möjlighet att utöva sin rätt till rättslig prövning inför en oavhängig och opartisk domstol för att erhålla tillgång till, rätta eller radera personuppgifter som rör dem"<sup>66</sup>. I samma sammanhang anser domstolen att ett effektivt rättsmedel mot sådana ingrepp inte enbart kan användas inför en domstol, utan även inför ett "organ"<sup>67</sup> som ger garantier som är väsentligen likvärdiga med dem som krävs enligt artikel 47 i stadgan. I Schrems II-domen betonade domstolen att domstolens eller organets oavhängighet ska säkerställas, särskilt i förhållande till den verkställande makten, med hjälp av alla nödvändiga garantier, inklusive vad gäller villkoren för att återkalla eller ogiltigförklara tillsättningen<sup>68</sup>, och att en domstols behörighet ska

---

<sup>59</sup> Europadomstolen, Sacharov, § 234.

<sup>60</sup> Europadomstolen, Kennedy, § 190.

<sup>61</sup> Europeiska dataskyddsstyrelsen noterar att Europarådets kommissarie för mänskliga rättigheter anser att den s.k. tredjepartsregeln – enligt vilken underrättelseorgan i ett land som lämnar uppgifter till underrättelseorgan i ett annat land kan införa en skyldighet för de mottagande organen att inte utlämna de överförda uppgifterna till en tredje part – inte bör gälla för tillsynsorgan, i syfte att inte undergräva möjligheten till effektivt rättsmedel (dokumentet *Democratic and effective oversight of national security services*).

<sup>62</sup> Europadomstolen, Kennedy, § 167.

<sup>63</sup> Ordet "tribunal" har till exempel översatts som "Gericht" på tyska och "gerecht" på nederländska.

<sup>64</sup> Artikel 13 i Europakonventionen.

<sup>65</sup> Europadomstolen, Klass, § 67.

<sup>66</sup> Se § 194 i Schrems II.

<sup>67</sup> Se § 197 i Schrems II, där domstolen uttryckligen använder detta ord.

<sup>68</sup> Se § 195 i Schrems II.

överensstämma med kraven i artikel 47 i stadgan. I detta avseende ska organet<sup>69</sup> vara behörigt att fatta bindande beslut i förhållande till underrättelsetjänsterna, i enlighet med rättsliga garantier som de registrerade skulle kunna göra gällande<sup>70</sup>.

#### 4. AVSLUTANDE ANMÄRKNINGAR

48. De fyra europeiska nödvändiga garantierna ska betraktas som centrala delar som bör konstateras vid bedömningar av nivån av ingrepp i de grundläggande rättigheterna till privatliv och dataskydd. Eftersom de är nära sammankopplade bör de inte bedömas separat utan snarare som en helhet, genom en kontroll av den relevanta lagstiftningen i förhållande till övervakningsåtgärderna, minimikraven för skydd av registrerades rättigheter samt rättsmedel som fastställs i tredjelandets nationella lagstiftning.

49. Dessa garantier kräver ett visst tolkningsarbete, särskilt eftersom tredjelandets lagstiftning inte behöver vara identisk med EU:s rättsliga ram.

50. Såsom Europadomstolen konstaterade i målet Kennedy beror en bedömning på ett falls alla omständigheter, till exempel de möjliga åtgärdernas art, räckvidd och varaktighet, skälen till att de förordnas, vilka myndigheter som är behöriga att godkänna, genomföra och övervaka dem, samt vilken typ av rättsmedel som föreskrivs i nationell lag<sup>71</sup>.

51. Följaktligen kan en bedömning av ett tredjelandets övervakningsåtgärder mot de europeiska nödvändiga garantierna leda till en av följande två slutsatser:

- ) Det berörda tredjelandets lagstiftning säkerställer inte kraven enligt de europeiska nödvändiga garantierna: I detta fall ger lagstiftningen i tredjelandet inte en skyddsnivå som är väsentligen likvärdig med den som garanteras inom EU.
- ) Det berörda tredjelandets lagstiftning uppfyller de europeiska nödvändiga garantierna.

52. När kommissionen bedömer om en adekvat skyddsnivå föreligger, i enlighet med artikel 45 i den allmänna dataskyddsförordningen, ska den avgöra om de europeiska nödvändiga garantierna är uppfyllda som en del av det som anses garantera att ett tredjelandets lagstiftning som helhet ger en skyddsnivå som är väsentligen likvärdig med den som garanteras inom EU.

53. När uppgiftsutförare och uppgiftsinförare vidtar lämpliga skyddsåtgärder i enlighet med artikel 46 i den allmänna dataskyddsförordningen, med hänsyn till de krav i tredjelandets lagstiftning som specifikt är tillämpliga på de överförda uppgifterna, ska de säkerställa att en väsentligen likvärdig skyddsnivå verkligen uppnås. Detta innebär framför allt att de, om tredjelandets lagstiftning inte överensstämmer med kraven enligt de europeiska nödvändiga garantierna, ska säkerställa att lagstiftningen i fråga inte inkräktar på de garantier och skyddsåtgärder som omger överföringen, så att en skyddsnivå som är väsentligen likvärdig med den som garanteras inom EU fortfarande kan uppnås.

---

<sup>69</sup> Se § 197 i Schrems II, där domstolen uttryckligen använder detta ord.

<sup>70</sup> Se § 196 i Schrems II.

<sup>71</sup> Europadomstolen, Kennedy, § 153.

54. Europeiska dataskyddsstyrelsen har utfärdat ytterligare riktlinjer och rekommendationer som ska beaktas vid bedömningen, beroende på vilket överföringsverktyg som ska användas och hur nödvändigt det är att införa lämpliga skyddsåtgärder, eventuellt också kompletterande åtgärder<sup>72</sup>.

55. Det bör dessutom noteras att de europeiska nödvändiga garantierna är baserade på vad som krävs i lag. Europeiska dataskyddsstyrelsen betonar att de europeiska nödvändiga garantierna är baserade på grundläggande rättigheter som gäller för alla, oavsett nationalitet.

56. Europeiska dataskyddsstyrelsen framhåller att de europeiska nödvändiga garantierna är en referensstandard vid bedömning av ingrepp som följer av övervakningsåtgärder i ett tredjeland i samband med internationella uppgiftsöverföringar. Denna standard grundar sig på EU-lagstiftningen och på rättspraxis från EU-domstolen och Europadomstolen, som är bindande för medlemsstaterna.

---

<sup>72</sup> Referensram för adekvat skyddsnivå, WP 254 rev. 01, reviderad och antagen den 6 februari 2018; Europeiska dataskyddsstyrelsen, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, den 10 november 2020.