Datainspektionen informerar

Nr 1/2018

Allmänna Råd

Datainspektionen ger ut allmänna råd i syfte:

1) Att öka personuppgiftsansvarigas och personuppgifts-biträdens medvetenhet om sina skyldigheter enligt EU:s dataskyddsförordning samt
2) Att öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling av personuppgifter.

De allmänna rådena är inte bindande, utan innehåller rekommendationer om hur de bindande kraven i dataskydds-förordningen kan uppnås. Detta dokument är en **allmän vägledning om inbyggt dataskydd och dataskydd som standard.** Inbyggt dataskydd och dataskydd som standard medför att informationssystemen uppfyller dataskydds-principerna och tar till vara de registrerades rättigheter. Vid utveckling av nya lösningar ska verksamheten tänka på data-skydd och informationssäkerhet. Att ta hänsyn till dataskyddet och informationssäkerheten genom systemets hela livscykel är både kostnadsbesparande och mer effektivt än att ändra i ett färdigutvecklat program.

Datainspektionen

den 29 mars 2018

1 Dataskyddet i offentlig sektor

Dataskydd är ett begrepp med många nyanser. Det finns ingen exakt eller bra definition på vad dataskydd är. Enkelt uttryckt handlar det om rätten till privatliv och rätten att bestämma över sina egna personuppgifter. Rätten till privatliv finns reglerat bland annat i den europeiska människorättskonventionen artikel 8 och ligger till grund för EU:s dataskyddsförordning[1] (GDPR).

I förhållandet mellan medborgare och offentlig sektor utgör dataskyddet även en garanti för rättsskydd. En medborgare med kontroll över de egna personuppgifterna kan motverka myndighetsmissbruk.

Offentlig sektor är en stor användare av alla typer av personuppgifter. Uppgifterna används ofta i sammanhang som har stora konsekvenser för den enskilda medborgarens rättigheter och skyldigheter. Därför är det viktigt att de uppgifter offentlig sektor behandlar är av god kvalitet.

Den tekniska utvecklingen ger möjligheter att utveckla och effektivisera behandlingen av personuppgifter.

Ur ett dataskyddsperspektiv är det viktigt att laggrundad tystnadsplikt inte åsidosätts eller begränsas på grund av de möjligheter tekniken ger.

För att säkra dataskyddet vid utbyte av och delning av personuppgifter mellan olika offentliga instanser, och mellan offentliga och privata aktörer ska ansvarsfördelningen vara tydlig. Det bör vara helt klart vilken instans som har ansvar för vad och vilken del av behandlingen.

För att den enskilda ska kunna bevaka sina rättigheter ska denne få information om var uppgifterna finns och för vilket ändamål de används.

Digitaliseringen öppnar upp för nya kommunikationsmöjligheter mellan offentlig sektor och privatpersoner eller verksamheter. När personuppgifter blir tillgängliga för den personuppgiftsansvariga är det viktigt att försäkra sig om att inte fler personuppgifter behandlas än vad som är nödvändigt för det specifika användningsändamålet. Rätten till privat kommunikation (kommunikationshemligheten) är en grundläggande rättighet. Kommunikationshemligheten gäller de som kommunicerar och inte vad som kommuniceras.

2 Dataskyddsprinciperna[2]

Respekten för privatlivet och den enskildes personliga integritet uppnås först när registrering av personuppgifter minimeras och användningen av personuppgifter begränsas till det som

[1] 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 upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

[2] Den personuppgiftsansvarige ska ansvara för och kunna visa att principerna efterlevs. Det innebär att det är inte tillräckligt med att följa EU:s dataskyddsförordning utan den personuppgiftsansvarige ska visa att förordningen följs

verkligen är nödvändigt. Utöver detta bör man grunda behandlingen på samtycke av den enskilda eller annan grund.

2.1 Rättsliga grunder

Myndighetsutövning kräver att personuppgifter behandlas oavsett den enskilde önskar det. Det kan till exempel gälla vid beskattning. I de fall behandlingen av personuppgifter inte grundar sig på samtycke ska det föreligga en annan rättslig grund.

2.2 Proportionalitet

All insamling av och vidare behandling av personuppgifter ska ske i enlighet med lagstiftningen eller på ett sätt som är rimligt i förhållande till den registrerade. Med det avses att behandlingen inte får medföra en orimlig belastning för den enskildes självbestämmanderätt eller integritet, att hänsyn till de olika inblandade parterna balanseras, och att registreringen ska vara proportionell i förhållande till ändamålet med behandlingen. I valet mellan två alternativa lösningar för behandling av personuppgifter ska det alternativ väljas som är minst integritetskränkande.

2.3 Ändamålsbegränsning

Personuppgifter får samlas in för ett visst på förhand bestämt ändamål. Ändamålet ska vara lagligt. Dessutom ska ändamålet för vidare behandling av personuppgifterna vara förenliga med det ändamål uppgifterna ursprungligen samlats in för. I konsekvens därmed ska personuppgifter inte heller överlåtas till andra utan att det föreligger samtycke eller en annan laglig grund för överlåtelsen.

2.4 Relevans och minimering

Personuppgifter ska bara inhämtas, lagras och behandlas i den utsträckning det är nödvändigt för att uppnå det lagliga ändamålet med behandlingen. Om det inte finns behov av att registrera personuppgifter ska det inte heller göras. Personuppgifter som inte längre är nödvändiga för det insamlade ändamålet ska raderas eller anonymiseras.

2.5 Korrekthet och fullständighet

Personuppgifterna ska vara relevanta, korrekta och fullständiga i förhållande till det ändamål de insamlats för. Det innebär att uppgifter som ligger till grund för behandling ska vara uppdaterade och tillräckliga och inte innehålla irrelevant information. Information som är lagrad i ett register ska ofta användas som underlag för att fatta beslut om de registrerade. Därför är det viktigt att besluten inte fattas på felaktiga eller ofullständiga grunder.

2.6 Information och insyn

Principen innebär en rätt för den registrerade att bli informerad om insamling och användning av personuppgifter. Det föreligger en rätt att kostnadsfritt få insyn i de uppgifter som är registrerade om en själv. Det ska också ges möjlighet att få felaktiga eller missvisande uppgifter raderade eller korrigerade. Dessutom har den registrerade rätt att under vissa förutsättningar få personlig kontakt med den personuppgiftsansvarige för att kunna uttrycka sin åsikt och bestrida beslutet då beslutet helt och hållet grundar sig på automatiserad behandling av

personuppgifter. Detta gäller i de fall där beslutet har väsentlig betydelse för den beslutet gäller.

2.7 Informationssäkerhet

De som lagrar personuppgifter ska vidta tillräckliga åtgärder för att skydda personuppgifterna mot obehörig tillgång, ändring, förstörelse eller spridning. Informationen ska också skyddas mot förstörelse som är förorsakad av en olyckshändelse.

2.8 Särskilt stränga bestämmelser vid behandling av särskilda kategorier känsliga personuppgifter

Vid behandlingen av känsliga personuppgifter gäller särskilt stränga bestämmelser. Dataskyddsförordningen (GDPR) definierar följande information som känslig:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse eller medlemskap i fackförening
- Behandling av genetiska uppgifter
- Behandling av biometriska uppgifter för att entydigt identifiera en fysisk person
- Uppgifter om hälsa
- Uppgifter om en fysisk persons sexualliv eller sexuella läggning

2.9 Anonymitet och behandling som inte går att spåra

Utgångspunkten är att all registrering ska noggrant övervägas. Om det inte är nödvändigt att registrera individrelaterade uppgifter har den enskilda rätt att vara anonym. Detta följer av att det ska finnas en rättslig grund för registrering och i enlighet med proportionalitetsprincipen. Den registrerade har rätt att kräva att den minst integritetskränkande åtgärden används för att uppnå ett på förhand bestämt ändamål med behandling av personuppgifter. Om ändamålet kan uppnås utan användning av uppgifter som går att identifiera individen så ska detta alternativ användas.

3 Principer för inbyggt dataskydd (Privacy by Design) och dataskydd som standard (Privacy by Default)

Det finns en skyldighet att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till riskerna för fysiska personers fri- och rättigheter. Inbyggt dataskydd eller privacy by design och dataskydd som standard (privacy by default) betyder att det tas hänsyn till dataskydd i alla utvecklingsfaser av ett system eller en lösning. Det är både kostnadsbesparande och mer effektivt än att ändra ett färdigt system.

3.1 Användarna kräver dataskydd

Gränserna mellan dataskydd, användarvänlighet och tillgänglighet blir allt otydligare. Användarna förväntar sig att IT-lösningar både är säkra och håller en hög dataskyddsnivå. Den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Läckor och missbruk av personuppgifter kan innebära bristande förtroende för den personuppgiftsansvarige. Det är viktigt att undvika bristande förtroende för myndigheter. Det har också visat sig vara dyrt att rätta fel och ändra lösningar efteråt.

3.2 Sju steg till inbyggt dataskydd

De sju stegen[3] är avsedda för den som beställer, kravställer, utformar, utvecklar, använder, avvecklar, är leverantör eller på annat sätt är involverad i att utveckla IT-verktyg som behandlar personuppgifter.

3.2.1 Var i framkant, förebygg hellre än att reparera

För en dataskyddsvänlig lösning är det viktigt att göra en riskvärderingsanalys så tidigt som möjligt i utvecklingsprocessen. Kostnaderna för att rätta fel och brister i ett färdigt system kan vara höga. Om du tar hänsyn till dataskyddet i ett tidigt skede av utvecklingen kan du undvika onödiga arbetsinsatser med att lindra bristande dataskydd efteråt. Exempel på kränkningar av integriteten kan vara bristande behörighetsstyrning, att det samlas in fler personuppgifter än vad som är nödvändigt samt läckage av och bristande radering av personuppgifter.

Exempel:

I en skola ska ett skoladministrationssystem utvecklas. Innan utvecklingen börjar görs det en analys av dataskyddskonsekvenserna (privacy impact assessment). Det handlar således om att göra en analys för att identifiera möjliga risker för dataskyddet. I konsekvensanalysen förutser man problem och föreslår lösningar. Med stöd av analysen kan ett system utvecklas som på bästa möjliga sätt tillvaratar elevernas, föräldrarnas och de anställdas dataskydd.

3.2.2 Gör dataskyddet till en standardinställning

Standardinställningen är beroende av vilket system som ska användas och vilken kategori av personuppgifter som ska lagras. För att ett system ska ha inbyggt dataskydd ska standardinställningarna göras så att inte fler personuppgifter än vad som är nödvändigt samlas in eller visas, att det finns ett specifikt ändamål med insamlingen, att det finns tekniska begränsningar gällande användningen av uppgifterna, att uppgifterna raderas när ändamålet har uppnåtts och att man bara får tillgång till de uppgifter som omfattas av den behörighet man tilldelats. Ett dylikt system kommer automatiskt att styra användaren till en arbetsprocess som ger ett bättre dataskydd.

Exempel:

En webbläsare är utvecklad med ”Do Not Track” som standardinställning. Det betyder att webbläsaren automatiskt ser till att användaren inte blir spårad. I de fall användaren vill att webbaktiviteten ska spåras kan han eller hon ändra inställningarna.

[3] De sju stegen till inbyggt dataskydd är fritt översatt och anpassat från ”7 foundational principles for privacy by design” by PH. D. Ann Cavoukian, Information & Privacy Commissioner in Ontario, Canada.

3.2.3 Bygg in dataskyddet i designen

Dataskyddet ska vara inbyggt i IT-systemets design och arkitektur samt användning. Det bör inte vara en funktion som läggs till efteråt. På detta sätt blir dataskyddet en viktig del av kärnverksamheten. Således blir dataskyddet en integrerad del av systemet utan att vara på bekostnad av funktionen.

Exempel:

Det är lätt att ge ifrån sig för mycket information om lösningen möjliggör det. För att undvika onödig insamling av personuppgifter kan webbaserade formulär, till exempel ett formulär som ska sändas till en hälsocentral förses med en färdig lista (dropplista) som ger valmöjligheter istället för att använda ett fritextfält.

3.2.4 Skapa full funktion: både och, inte alls-eller

Genom inbyggt dataskydd tar verksamheten tillvara användarens dataskydd och de egna behoven. Det är viktigt att ta hänsyn till dataskyddet från början för att undgå reparationer som går utöver funktionen. Ibland är det inte möjligt att göra ändringar efteråt utan att försämra systemet. Målet är både- och (”win-win”) framom en inte alls-eller för att ta till vara verksamhetens behov och samtidigt ta hänsyn till de registrerades dataskydd.

Exempel:

En kund ringer till telefonoperatören från sitt registrerade telefonnummer. Systemet styr om så att den kundansvariga automatiskt får tillgång till de uppgifter som är registrerade om kunden. Den som behandlar kundens uppgifter har tillgång till de aktuella uppgifterna utan att se resten av kundregistret (processen i systemet är tillgångsstyrd).

3.2.5 Ta tillvara informationssäkerheten från början till slutet

Informationssäkerheten[4] är en del av lösningen genom systemets hela livscykel - från förstudie via design och utveckling till användning och avveckling. Det betyder att allt som sker i systemet är riskanalyserat och säkrat, allt från och med att personuppgifterna samlas in, medan de behandlas och till dess de raderats. Personuppgifterna ska säkras mot otillåten användning, ändring, förstörelse och spridning.

Exempel:

Ett system är byggt för att följa säkerhetsstandarder för att säkra personuppgifternas konfidentialitet, integritet och tillgänglighet genom hela livscykeln. Det inkluderar metoder för säker radering, kryptering, stark behörighetskontroll och loggning. Systemet ska kunna samla in

[4] Informationssäkerhet bidrar till att säkra uppgifterna, systemet och annat mot till exempel intrång, otillåten delning eller tillgång till uppgifterna.

de mest nödvändiga personuppgifterna. Systemet innehåller dessutom rutiner för automatisk radering av data när de inte längre behövs.

3.2.6 Viss öppenhet

Öppenhet om på vilket sätt dataskyddet är ordnat ska gälla beträffande systemen. Verksamheten ska se till att användarna får tillräcklig information och att det finns möjlighet att få insyn i hur de egna personuppgifterna behandlas. Det ska vara möjligt att kontrollera att systemet tillvaratar dataskyddet på det sätt som leverantören uppger.

Exempel:

I en e-handelslösning informeras kunden om vilka av dennes uppgifter som behandlas i lösningen. Informationen ges genom en bra och användarvänlig dataskyddsbeskrivning som är lätt tillgänglig för kunden, både då denne registrerar sig, men också efter att denne har registrerat sig. Kunden blir informerad om vilken information som samlas in, hur den används, vem som har tillgång till den, hur länge informationen lagras, kundens möjligheter att ändra och radera uppgifterna och vilka andra instanser uppgifterna lämnas till.

3.2.7 Respekt för användarnas dataskydd

Framför allt kräver inbyggt dataskydd[5] att utvecklarna, beställarna och administratörerna ger användarnas dataskydd hög prioritet. Det kan göras genom att dataskyddet tas till vara genom standardinställningar, tydliga användarvillkor och lösningar för att användaren ska kunna kontrollera sina egna personuppgifter.

[5] Läs mer och se checklista för inbyggt dataskydd på

http://www.di.ax/sites/default/files/attachments/page/allmanna_rad_nr_4_2012_dnr_16_2012_privacy_bydesign.pdf

Bilaga

Utdrag ur 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 (allmän dataskydds-förordning)

Artikel 4

Definitioner

I denna förordning avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

3. *begränsning av behandling*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,

4. *profilering*: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar,

5. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person,

6. *register*: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

7. *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller

medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt,

8. *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

9. *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte,

10. *tredje part*: en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna,

11. *samtycke* av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne,

12. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

13. *genetiska uppgifter*: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga,

14. *biometriska uppgifter*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter,

15. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,

16. *huvudsakligt verksamhetsställe*:

    a) när det gäller en personuppgiftsansvarig med verksamhetsställen i mer än en medlemsstat, den plats i unionen där vederbörande har sin centrala förvaltning, om inte besluten om ändamålen och medlen för behandlingen av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen och det sistnämnda verksamhetsstället har befogenhet att få sådana beslut genomförda, i vilket fall det verksamhetsställe som har fattat sådana beslut ska betraktas som det huvudsakliga verksamhetsstället,

    b) när det gäller ett personuppgiftsbiträde med verksamhetsställen i mer än en medlemsstat, den plats i unionen där vederbörande har sin centrala förvaltning eller, om personuppgiftsbiträdet inte har någon central förvaltning i unionen, det av personuppgiftsbiträdets verksamhetsställen i

unionen där den huvudsakliga behandlingen inom ramen för verksamheten vid ett av personuppgiftsbiträdets verksamhetsställen sker, i den utsträckning som personuppgiftsbiträdet omfattas av särskilda skyldigheter enligt denna förordning,

17. *företrädare*: en i unionen etablerad fysisk eller juridisk person som skriftligen har utsetts av den personuppgiftsansvarige eller personuppgiftsbiträdet i enlighet med artikel 27 och företräder denne i frågor som gäller dennes skyldigheter enligt denna förordning,

18. *företag*: en fysisk eller juridisk person som bedriver ekonomisk verksamhet, oavsett dess juridiska form, vilket inbegriper partnerskap eller föreningar som regelbundet bedriver ekonomisk verksamhet,

19. *koncern*: ett kontrollerande företag och dess kontrollerade företag,

20. *bindande företagsbestämmelser*: strategier för skydd av personuppgifter som en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad på en medlemsstats territorium använder sig av vid överföringar eller en uppsättning av överföringar av personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett eller flera tredjeländer inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet,

21. *tillsynsmyndighet*: en oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 51,

22. *berörd tillsynsmyndighet*: en tillsynsmyndighet som berörs av behandlingen av personuppgifter på grund av att

    a) den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad på tillsynsmyndighetens medlemsstats territorium,

    b) registrerade som är bosatta i den tillsynsmyndighetens medlemsstat i väsentlig grad påverkas eller sannolikt i väsentlig grad kommer att påverkas av behandlingen, eller

    c) ett klagomål har lämnats in till denna tillsynsmyndighet,

23. *gränsöverskridande behandling*:

    a) behandling av personuppgifter som äger rum inom ramen för verksamhet vid verksamhetsställen i mer än en medlemsstat tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen, när den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller

    b) behandling av personuppgifter som äger rum inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen men som i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat,

24. *relevant och motiverad invändning*: en invändning mot ett förslag till beslut avseende frågan huruvida det föreligger en överträdelse av denna förordning eller huruvida den planerade åtgärden i förhållande till den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med denna förordning, av vilken invändning det tydligt framgår hur stora risker utkastet till beslut medför när det gäller registrerades grundläggande rättigheter och friheter samt i tillämpliga fall det fria flödet av personuppgifter inom unionen,

25. *informationssamhällets tjänster*: alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([1]),

26. *internationell organisation*: en organisation och dess underställda organ som lyder under folkrätten, eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder.

KAPITEL II

Principer

Artikel 5

Principer för behandling av personuppgifter

1.Vid behandling av personuppgifter ska följande gälla:

a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (*laglighet, korrekthet och öppenhet*).

b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (*ändamålsbegränsning*).

c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).

d) De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (*korrekthet*).

([1]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (*lagringsminimering*).

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).

2.Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (*ansvarsskyldighet*).

Artikel 6

Laglig behandling av personuppgifter

1. Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Led f i första stycket ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

2.Medlemsstaterna får behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning med hänsyn till behandling för att efterleva punkt 1 c och e genom att närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling, inbegripet för andra specifika situationer då uppgifter behandlas i enlighet med kapitel IX.

3.Den grund för behandlingen som avses i punkt 1 c och e ska fastställas i enlighet med

a) unionsrätten, eller

b) en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av.

Syftet med behandlingen ska fastställas i den rättsliga grunden eller, i fråga om behandling enligt punkt 1 e, ska vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning, bland annat: de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för

behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling, däribland för behandling i andra särskilda situationer enligt kapitel IX. Unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

4.Om en behandling för andra ändamål än det ändamål för vilket personuppgifterna samlades in inte grundar sig på den registrerades samtycke eller på unionsrätten eller medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1, ska den personuppgiftsansvarige för att fastställa huruvida behandling för andra ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in bland annat beakta följande:

a)Kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen.

b)Det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige.

c)Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas i enlighet med artikel 9 eller huruvida personuppgifter om fällande domar i brottmål och överträdelser behandlas i enlighet med artikel 10.

d)Eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen.

e)Förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering.

Artikel 7

Villkor för samtycke

1.Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter.

2.Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Om en del av förklaringen innebär en överträdelse av denna förordning, ska denna del inte vara bindande.

3.De registrerade ska ha rätt att när som helst återkalla sitt samtycke. Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycke, innan detta återkallas. Innan samtycke lämnas ska den registrerade informeras om detta. Det ska vara lika lätt att återkalla som att ge sitt samtycke.

4.Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn bland annat tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.