Riktlinjer

Riktlinjer 4/2019 om artikel 25

Inbyggt dataskydd och dataskydd som standard

Version 2.0

Antagna den 20 oktober 2020

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

Versionshistorik

Version 1.0	13 november 2019	Antagande av riktlinjerna inför offentligt samråd
Version 2.0	20 oktober 2020	EDPB:s antagande av riktlinjerna efter offentligt samråd

Innehållsförteckning

Europeiska dataskyddsstyrelsen har

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 *dataskyddsförordningen*),

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

med beaktande av artikel 12 och artikel 22 i arbetsordningen,

ANTAGIT FÖLJANDE RIKTLINJER.

Sammanfattning

I en värld som blir alltmer digitaliserad spelar efterlevnaden av kraven på inbyggt dataskydd och dataskydd som standard en viktig roll för att främja integritet och dataskydd i samhället. Det är därför viktigt att personuppgiftsansvariga tar detta ansvar på allvar och genomför skyldigheterna i dataskyddsförordningen när de utformar behandlingen.

I dessa riktlinjer ges allmän vägledning om de skyldigheter i fråga om inbyggt dataskydd och dataskydd som standard som anges i artikel 25 i dataskyddsförordningen. Inbyggt dataskydd och dataskydd som standard är en skyldighet som alla personuppgiftsansvariga måste uppfylla, oavsett hur omfattande eller komplicerad behandlingen är. För att kunna genomföra kraven på inbyggt dataskydd och dataskydd som standard är det viktigt att den personuppgiftsansvarige förstår principerna för dataskydd och den registrerades rättigheter och friheter.

Den huvudsakliga skyldigheten är att vidta *lämpliga* åtgärder och nödvändiga skyddsåtgärder som säkerställer ett *effektivt genomförande* av *principerna för dataskydd* och följaktligen *de registrerades rättigheter och friheter genom inbyggt dataskydd och dataskydd som standard*. I artikel 25 föreskrivs både inbyggda faktorer och standardfaktorer som ska beaktas. Dessa aspekter kommer att utvecklas ytterligare i dessa riktlinjer.

I artikel 25.1 föreskrivs att personuppgiftsansvariga bör överväga inbyggt dataskydd och dataskydd som standard i ett tidigt skede av sin planering för ny behandling. Personuppgiftsansvariga ska genomföra inbyggt dataskydd och dataskydd som standard *före* behandlingen och *fortsätta* med detta under behandlingen, genom att regelbundet granska hur effektiva de valda åtgärderna och skyddsåtgärderna är. Inbyggt dataskydd och dataskydd som standard gäller även för befintliga system för behandling av personuppgifter.

Riktlinjerna innehåller även vägledning om hur principerna för dataskydd i artikel 5 kan genomföras på ett effektivt sätt, med angivande av central utformning och standardelement samt praktiska exempel som illustration. Den personuppgiftsansvarige bör överväga om de föreslagna åtgärderna är lämpliga för just den aktuella behandlingen.

Europeiska dataskyddsstyrelsen (EDPB) ger rekommendationer om hur personuppgiftsansvariga, personuppgiftsbiträden och producenter kan samarbeta för att uppnå inbyggt dataskydd och

dataskydd som standard. EDPB uppmuntrar personuppgiftsansvariga inom industrin, personuppgiftsbiträden och producenter att använda inbyggt dataskydd och dataskydd som standard som ett sätt att få en konkurrensfördel när de marknadsför sina produkter till personuppgiftsansvariga och de registrerade. EDPB uppmanar även alla personuppgiftsansvariga att använda certifieringar och uppförandekoder.

1 TILLÄMPNINGSOMRÅDE

1. Riktlinjerna fokuserar på de personuppgiftsansvarigas genomförande av inbyggt dataskydd och dataskydd som standard på grundval av skyldigheten i artikel 25 i dataskyddsförordningen.[1] Dessa riktlinjer kan även vara användbara för andra aktörer, såsom personuppgiftsbiträden och producenter av produkter, tjänster och applikationer (nedan kallade *producenter*), som inte uttryckligen anges i artikel 25, när de skapar produkter och tjänster som uppfyller kraven i dataskyddsförordningen och som gör det möjligt för personuppgiftsansvariga att fullgöra sina skyldigheter avseende dataskydd.[2] I skäl 78 i dataskyddsförordningen anges dessutom att inbyggt dataskydd och dataskydd som standard bör beaktas vid offentliga upphandlingar. Trots att alla personuppgiftsansvariga har en skyldighet att integrera inbyggt dataskydd och dataskydd som standard i sin behandling av personuppgifter främjar denna bestämmelse antagandet av principerna för dataskydd, där offentliga förvaltningar bör föregå med gott exempel. Den personuppgiftsansvarige ansvarar för att skyldigheterna avseende inbyggt dataskydd och dataskydd som standard fullgörs vid den behandling som utförs av deras personuppgiftsbiträden och underleverantörer , och bör därför ta hänsyn till detta när de ingår avtal med dessa parter.

2. Det krav som beskrivs i artikel 25 innebär att personuppgiftsansvariga ska bygga in dataskyddet i behandlingen av personuppgifter och ha detta som en standardinställning, och att detta ska gälla under hela behandlingen. Kravet på inbyggt dataskydd och dataskydd som standard gäller också för de behandlingssystem som fanns innan dataskyddsförordningen trädde i kraft. Personuppgiftsansvariga måste konsekvent uppdatera behandlingen i enlighet med dataskyddsförordningen. För mer information om hur man ser till att ett befintligt system följer dataskyddsförordningen, se avsnitt 2.1.4 i dessa riktlinjer. Bestämmelsens huvudsyfte är att säkerställa ett *lämpligt* och *effektivt* dataskydd både genom *inbyggt* dataskydd och genom dataskydd som *standard*, vilket innebär att personuppgiftsansvariga bör kunna visa att de har vidtagit lämpliga åtgärder och skyddsåtgärder vid behandlingen för att säkerställa att principerna för dataskydd och de registrerades rättigheter och friheter är verkningsfulla.

3. I kapitel 2 i riktlinjerna ligger fokus på tolkningen av de krav som föreskrivs i artikel 25, och i samma kapitel behandlas de rättsliga förpliktelser som införts genom den bestämmelsen. I kapitel 3 ges exempel på hur inbyggt dataskydd och dataskydd som standard ska tillämpas i samband med särskilda principer för dataskydd.

[1] De tolkningar som tillhandahålls här är även tillämpliga på artikel 20 i direktiv (EU) 2016/680 och artikel 27 i förordning 2018/1725.

[2] I skäl 78 i dataskyddsförordningen anges detta behov tydligt: *”Vid utveckling, utformning, urval och användning av applikationer, tjänster och produkter som är baserade på behandling av personuppgifter eller behandlar personuppgifter för att uppfylla sitt syfte bör producenterna av dessa produkter, tjänster och applikationer uppmanas att beakta rätten till dataskydd när sådana produkter, tjänster och applikationer utvecklas och utformas och att, med tillbörlig hänsyn till den tekniska utvecklingen, säkerställa att personuppgiftsansvariga och personuppgiftsbiträden kan fullgöra sina skyldigheter avseende dataskydd.”*

4. I kapitel 4 i riktlinjerna behandlas möjligheten att inrätta en certifieringsmekanism för att visa överensstämmelse med artikel 25, och i kapitel 5 beskrivs hur tillsynsmyndigheter kan kontrollera efterlevnaden av den artikeln. Slutligen ger dessa riktlinjer berörda aktörer ytterligare rekommendationer om hur inbyggt dataskydd och dataskydd som standard kan genomföras på ett framgångsrikt sätt. EDPB inser vilka utmaningar små och medelstora företag står inför när det gäller att uppfylla alla skyldigheter avseende inbyggt dataskydd och dataskydd som standard, och därför innehåller kapitel 6 ytterligare rekommendationer till just små och medelstora företag.

2 ANALYS AV ARTIKEL 25.1 OCH 25.2 OM INBYGGT DATASKYDD OCH DATASKYDD SOM STANDARD

5. Syftet med detta kapitel är att utreda och ge vägledning avseende kraven på inbyggt dataskydd i artikel 25.1 i dataskyddsförordningen, respektive dataskydd som standard i artikel 25.2 i dataskyddsförordningen. Inbyggt dataskydd och dataskydd som standard är kompletterande begrepp som ömsesidigt förstärker varandra. De registrerade kommer att gynnas ännu mer av dataskydd som standard om det samtidigt finns inbyggt dataskydd – och vice versa.

6. Inbyggt dataskydd och dataskydd som standard är ett krav för alla personuppgiftsansvariga, och gäller både småföretag och multinationella företag. Hur svårt det blir att genomföra inbyggt dataskydd och dataskydd som standard kan därför variera beroende på behandlingen i det enskilda fallet. Oavsett storlek kan dock genomförandet av inbyggt dataskydd och dataskydd som standard gynna både den personuppgiftsansvarige och den registrerade.

2.1 Artikel 25.1: Inbyggt dataskydd

2.1.1 Den personuppgiftsansvariges skyldighet att genomföra lämpliga tekniska och organisatoriska åtgärder och nödvändiga skyddsåtgärder i behandlingen

7. I enlighet med artikel 25.1 ska den personuppgiftsansvarige genomföra *lämpliga* tekniska och organisatoriska *åtgärder* som är utformade för att genomföra principerna för dataskydd och integrera de *nödvändiga skyddsåtgärderna* i behandlingen för att uppfylla kraven och skydda de registrerades rättigheter och friheter. Både lämpliga åtgärder och nödvändiga skyddsåtgärder har samma syfte, nämligen att skydda de registrerades rättigheter och sörja för att skyddet av deras personuppgifter byggs in i behandlingen.

8. *Tekniska och organisatoriska åtgärder* och nödvändiga *skyddsåtgärder* ska tolkas i vid mening som samtliga metoder eller medel som en personuppgiftsansvarig kan använda vid behandlingen. För att vara *lämpliga* bör åtgärderna och de nödvändiga skyddsåtgärderna vara lämpade för att uppnå det avsedda syftet, dvs. de måste genomföra principerna för dataskydd *på ett effektivt sätt*[3]. Lämplighetskravet har således ett nära samband med kravet på effektivitet.

9. En teknisk eller organisatorisk åtgärd och en skyddsåtgärd kan vara allt från användning av avancerade tekniska lösningar till grundläggande utbildning av personalen. Beroende på sammanhanget och de risker som är förbundna med den aktuella behandlingen kan exempel vara pseudonymisering av personuppgifter[4], lagring av personuppgifter i ett strukturerat, allmänt använt maskinläsbart format, möjliggörande för de registrerade att ingripa i behandlingen, tillhandahållande av information om

[3] Kravet på effektivitet behandlas nedan i avsnitt 2.1.2.
[4] Definieras i artikel 4.5 i dataskyddsförordningen.

lagringen av personuppgifter, disponerande av system som upptäcker sabotageprogram, utbildning av personal i grundläggande ”it-hygien”, inrättande av system för hantering av integritet och informationssäkerhet, avtalsenliga förpliktelser för personuppgiftsbiträden att genomföra särskild praxis för uppgiftsminimering etc.

10. Standarder, bästa praxis och uppförandekoder som erkänns av sammanslutningar och andra organ som företräder olika kategorier av personuppgiftsansvariga kan vara till hjälp vid fastställandet av lämpliga åtgärder. Den personuppgiftsansvarige måste dock kontrollera att åtgärderna är lämpliga för den aktuella behandlingen.

2.1.2 Utformade för att effektivt genomföra principerna för dataskydd samt skydda de registrerades rättigheter och friheter

11. *Principerna för dataskydd* anges i artikel 5 (nedan kallade *principerna*). De *registrerades rättigheter och friheter* är fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, vilket i artikel 1.2 anges som syftet med dataskyddsförordningen (nedan kallade *rättigheterna*)[5]. Den exakta lydelsen av dessa rättigheter anges i EU-stadgan om de grundläggande rättigheterna. Den personuppgiftsansvarige måste förstå vad *principerna* och *rättigheterna* innebär för det skydd som dataskyddsförordningen ger, särskilt skyldigheten avseende inbyggt dataskydd och dataskydd som standard.

12. Vid genomförandet av lämpliga tekniska och organisatoriska åtgärder bör åtgärderna och skyddsåtgärderna vara *utformade* så att var och en av de ovannämnda principerna och det efterföljande skyddet av rättigheter kan genomföras på ett effektivt sätt.

Redogörelse för effektivitetskravet

13. Effektiviteten spelar en central roll för begreppet inbyggt dataskydd. Kravet på ett effektivt genomförande av principerna innebär att personuppgiftsansvariga måste vidta nödvändiga åtgärder och skyddsåtgärder för att skydda dessa principer, i syfte att säkerställa de registrerades rättigheter. Varje åtgärd som genomförs bör ge de avsedda resultaten för den behandling som den personuppgiftsansvarige planerar. Denna iakttagelse får två konsekvenser.

14. För det första innebär detta att artikel 25 inte innehåller krav på specifika tekniska och organisatoriska åtgärder, utan snarare att de valda åtgärderna och skyddsåtgärderna bör utformas för genomförandet av principerna för dataskydd i just den aktuella behandlingen. Åtgärderna och skyddsåtgärderna bör därför utformas på ett robust sätt, och den personuppgiftsansvarige bör kunna ta till ytterligare åtgärder för att möta ökade risker[6]. Frågan huruvida åtgärder är effektiva beror därför på omständigheterna i samband med behandlingen i det enskilda fallet och på en bedömning av vissa omständigheter som bör beaktas vid fastställandet av medlen för behandlingen. Dessa omständigheter behandlas nedan i avsnitt 2.1.3.

[5] Se skäl 4 i dataskyddsförordningen.

[6] Grundläggande principer som är tillämpliga på personuppgiftsansvariga (dvs. legitimitet, uppgiftsminimering, ändamålsbegränsning, öppenhet, dataintegritet samt att uppgifterna är korrekta) bör inte påverkas, oberoende av vilken behandling det är fråga om och riskerna för de registrerade. Emellertid har vederbörlig hänsyn till arten och omfattningen av en sådan behandling alltid utgjort en integrerad del av tillämpningen av dessa principer, så att de i sig är skalbara. Artikel 29-gruppen. ”Statement on the role of a risk-based approach in data protection legal frameworks”, WP 218, 30 maj 2014, s. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

15. För det andra bör personuppgiftsansvariga kunna visa att principerna har iakttagits.

16. De genomförda åtgärderna och skyddsåtgärderna bör uppnå önskad effekt i fråga om dataskydd, och den personuppgiftsansvarige bör kunna dokumentera de tekniska och organisatoriska åtgärder som genomförts.[7] För att göra detta får den personuppgiftsansvarige fastställa lämpliga nyckelutförandeindikatorer för att visa på effektivitet. En nyckelutförandeindikator är ett mätbart värde som valts av den personuppgiftsansvarige och som visar hur effektivt den personuppgiftsansvarige uppnår sitt dataskyddsmål. Nyckelutförandeindikatorer kan vara *kvantitativa*, såsom procentandelen falska positiva och falska negativa resultat, minskning av antalet klagomål eller minskad svarstid när de registrerade utövar sina rättigheter, eller *kvalitativa*, såsom utvärderingar av genomförandet, användning av betygsskalor eller expertutlåtanden. Som ett alternativ till nyckelutförandeindikatorerna kan personuppgiftsansvariga eventuellt visa att principerna genomförs på ett effektivt sätt genom att redogöra för logiken bakom sin bedömning av effektiviteten hos de valda åtgärderna och skyddsåtgärderna.

2.1.3 Omständigheter som ska beaktas

17. I artikel 25.1 anges vilka omständigheter som den personuppgiftsansvarige ska beakta vid fastställandet av åtgärderna i samband med en specifik behandling. Nedan ges vägledning om hur dessa omständigheter ska tillämpas i utformningsprocessen, vilket även omfattar utformningen av standardinställningar. Alla dessa omständigheter bidrar till att avgöra om en åtgärd är lämplig för att genomföra principerna på ett effektivt sätt. De utgör således inte ett mål i sig utan faktorer som ska beaktas tillsammans för att uppnå målet.

2.1.3.1 Den senaste utvecklingen

18. Begreppet ”den senaste utvecklingen” finns i flera EU-regelverk, t.ex. i samband med miljöskydd och produktsäkerhet. I dataskyddsförordningen hänvisas inte enbart till den senaste utvecklingen[8] i artikel 32 om säkerhetsåtgärder,[9] [10] utan även i artikel 25, vilket således innebär att detta riktmärke gäller för alla tekniska och organisatoriska åtgärder som är inbyggda i behandlingen.

19. I samband med artikel 25 medför hänvisningen till den senaste utvecklingen en skyldighet för personuppgiftsansvariga **att beakta de aktuella framsteg på teknikområdet** som är tillgängliga på marknaden vid fastställandet av lämpliga tekniska och organisatoriska åtgärder. Kravet är att personuppgiftsansvariga ska ha kunskap om och hålla sig uppdaterade om tekniska framsteg, om hur teknik kan medföra datasäkerhetsrisker eller möjligheter för behandlingen och om hur de åtgärder och skyddsåtgärder som säkerställer *ett effektivt genomförande* av principerna och de registrerades rättigheter ska genomföras och uppdateras.

---

[7] Se skälen 74 och 78.

[8] Se den tyska federala författningsdomstolens avgörande i målet Kalkar från 1978: https://germanlawarchive.iuscomp.org/?p=67, som kan tillhandahålla en grund för en metod för en objektiv definition av begreppet. Mot denna bakgrund skulle den senaste utvecklingens tekniska nivå fastställas mellan den tekniska nivån för ”den befintliga vetenskapliga kunskapen och forskningen” och de mer etablerade ”allmänt accepterade tekniska reglerna”. Den senaste utvecklingen kan således fastställas som den tekniska nivån på en tjänst, teknik eller produkt som finns på marknaden och är mest effektiv för att uppnå de fastställda målen.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

20. Den senaste utvecklingen är ett dynamiskt begrepp som statistiskt sett inte kan definieras vid en fastställd tidpunkt, utan som bör bedömas *kontinuerligt* i förhållande till den tekniska utvecklingen. Mot bakgrund av den tekniska utvecklingen kan en personuppgiftsansvarig upptäcka att en åtgärd som en gång tillhandahöll en adekvat skyddsnivå inte längre gör det. Underlåtenhet att hålla sig uppdaterad när det gäller tekniska förändringar kan därför medföra bristande överensstämmelse med artikel 25.

21. Kravet på beaktande av den senaste utvecklingen är tillämpligt både på tekniska och organisatoriska åtgärder. Avsaknad av lämpliga organisatoriska åtgärder kan minska eller till och med helt undergräva effektiviteten hos en vald teknik. Exempel på organisatoriska åtgärder är antagande av interna policyer, uppdaterad utbildning i teknik, säkerhet och dataskydd och policyer för styrning och förvaltning av it-säkerhet.

22. Befintliga och erkända ramar, standarder, certifieringar, uppförandekoder osv. inom olika områden kan spela en roll när det gäller att ange den aktuella senaste tekniken inom det aktuella användningsområdet. Om sådana standarder finns och ger en hög skyddsnivå för den registrerade i enlighet med – eller som går utöver – de lagstadgade kraven bör personuppgiftsansvariga ta hänsyn till dessa vid utformningen och genomförandet av dataskyddsåtgärder.

2.1.3.2 Genomförandekostnader

23. Den personuppgiftsansvarige får ta hänsyn till kostnaderna för genomförandet när han eller hon väljer och tillämpar lämpliga tekniska och organisatoriska åtgärder och nödvändiga skyddsåtgärder som effektivt genomför principerna för att skydda de registrerades rättigheter. Kostnaderna hänför sig till resurser i allmänhet, inbegripet tid och personal.

24. Kostnadsaspekten innebär inte att den personuppgiftsansvarige måste spendera en oproportionerligt stor mängd resurser när alternativa, mindre resurskrävande men ändå effektiva åtgärder finns. Genomförandekostnaderna är dock en faktor som bör beaktas vid genomförandet av inbyggt dataskydd snarare än som en grund för att inte genomföra detta skydd.

25. De valda åtgärderna ska således säkerställa att den personuppgiftsansvariges planerade behandling inte omfattar behandling av personuppgifter som strider mot principerna, oberoende av kostnad. Personuppgiftsansvariga bör kunna hantera de totala kostnaderna för att på ett effektivt sätt kunna genomföra alla principer och därmed skydda rättigheterna.

2.1.3.3 Behandlingens art, omfattning, sammanhang och ändamål

26. Personuppgiftsansvariga måste ta hänsyn till behandlingens art, omfattning, sammanhang och ändamål när de fastställer nödvändiga åtgärder.

27. Dessa faktorer bör tolkas i överensstämmelse med deras roll i andra bestämmelser i dataskyddsförordningen, såsom artiklarna 24, 32 och 35, i syfte att låta principerna för dataskydd bli en del av behandlingen.

28. Begreppet **art** kan kortfattat uttryckt förstås som behandlingens inneboende[11] egenskaper. **Omfattningen** avser behandlingens storlek och räckvidd. **Sammanhanget** hänför sig till

[11] Exempel på detta är särskilda kategorier av personuppgifter, automatiskt beslutsfattande, skeva maktförhållanden, oförutsägbar behandling, svårigheter för den registrerade att utöva sina rättigheter osv.

omständigheterna vid behandlingen, vilka kan påverka den registrerades förväntningar, medan **ändamålet** avser behandlingens syfte.

2.1.3.4 Riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter

29. Många av bestämmelserna i dataskyddsförordningen, till exempel artiklarna 24, 25, 32 och 35, bygger på ett enhetligt riskbaserat tillvägagångssätt i syfte att identifiera lämpliga tekniska och organisatoriska åtgärder för att skydda enskilda och deras personuppgifter och uppfylla kraven i dataskyddsförordningen. De tillgångar som ska skyddas är alltid desamma (enskilda, genom skyddet av deras personuppgifter), samma risker ska motverkas (beträffande enskildas rättigheter), och samma villkor ska beaktas (behandlingens art, omfattning, sammanhang och ändamål).

30. Vid genomförandet av den riskanalys som krävs för efterlevnad av artikel 25 måste den personuppgiftsansvarige identifiera de risker för de registrerades rättigheter som en överträdelse av principerna innebär, och fastställa deras sannolikhet och allvar så att han eller hon kan vidta åtgärder för att effektivt minska de identifierade riskerna. En systematisk och grundlig utvärdering av behandlingen är avgörande vid genomförandet av riskbedömningar. En personuppgiftsansvarig bedömer exempelvis de särskilda risker som är förknippade med avsaknad av frivilligt samtycke, vilket utgör en överträdelse av legalitetsprincipen, i samband med behandling av personuppgifter avseende en utsatt grupp som barn och ungdomar under 18 år, om det inte finns någon annan rättslig grund, och genomför lämpliga åtgärder för att hantera och effektivt minska de identifierade risker som förknippas med denna grupp av registrerade.

31. Vägledning om hur dataskyddsrisker ska bedömas och om hur en bedömning av dataskyddsrisker ska genomföras tillhandahålls i EDPB:s riktlinjer om konsekvensbedömning avseende dataskydd[12], där fokus ligger på fastställande av huruvida en behandling sannolikt leder till en hög risk för den registrerade. Dessa riktlinjer kan även vara användbara vid riskbedömningen i samtliga artiklar som anges ovan, inbegripet artikel 25.

32. Det riskbaserade tillvägagångssättet utesluter inte användning av utgångsvärden, bästa praxis och standarder. Dessa kan vara ändamålsenliga verktyg för personuppgiftsansvariga när de hanterar liknande risker i liknande situationer (behandlingens art, omfattning, sammanhang och ändamål). Emellertid kvarstår skyldigheten enligt artikel 25 (samt artiklarna 24, 32 och 35.7 c) att beakta *”riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter*”. Därför är personuppgiftsansvariga, trots att de stöds av sådana verktyg, alltid skyldiga att göra en riskbedömning i varje enskilt fall, och verifiera huruvida de lämpliga åtgärder och skyddsåtgärder som har föreslagits är effektiva. Det kan dessutom senare behöva göras en konsekvensbedömning avseende dataskydd, eller en uppdatering av en befintlig konsekvensbedömning avseende dataskydd.

2.1.4 Tidsaspekt

2.1.4.1 Vid fastställandet av vilka medel behandlingen utförs med

33. Inbyggt dataskydd ska genomföras *”vid fastställandet av vilka medel behandlingen utförs med”.*

[12] Artikel 29-gruppens riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning (EU) 2016/679, WP 248 rev.01, 4 oktober 2017, ec.europa.eu/newsroom/document.cfm?doc_id=47711 – godkända av EDPB.

34. *”Vilka medel behandlingen utförs med”* varierar från allmänna till detaljerade delar av utformningen av behandlingen, såsom dess struktur, förfaranden, protokoll, layout och utseende.

35. Med *”tidpunkten för fastställandet av vilka medel behandlingen utförs med”* avses den tidsperiod då den personuppgiftsansvarige beslutar hur behandlingen ska utföras och på vilket sätt behandlingen ska ske och vilka mekanismer som ska användas för att utföra behandlingen. Det är under arbetet med att fatta sådana beslut som den personuppgiftsansvarige är skyldig att bedöma de lämpliga åtgärderna och skyddsåtgärderna för att principerna och de registrerades rättigheter ska genomföras på ett effektivt sätt i behandlingen, och beakta faktorer såsom den senaste utvecklingen, genomförandekostnader, art, omfattning, sammanhang och ändamål samt risker. Detta inbegriper tidpunkten för upphandling och implementering av programvara, maskinvara och tjänster för databehandling.

36. Att redan i ett tidigt skede överväga inbyggt dataskydd och dataskydd som standard är avgörande för ett framgångsrikt genomförande av principerna och skyddet av de registrerades rättigheter. Ur ett kostnads–nyttoperspektiv ligger det dessutom i de personuppgiftsansvarigas intresse att beakta inbyggt dataskydd och dataskydd som standard så tidigt som möjligt, eftersom det kan vara krävande och dyrt att ändra redan uppgjorda planer och redan utformade behandlingar.

2.1.4.2 Vid själva behandlingen (upprätthållande och översyn av dataskyddskrav)

37. När behandlingen har inletts är den personuppgiftsansvarige fortsatt skyldig att upprätthålla inbyggt dataskydd och dataskydd som standard, dvs. fortsätta att på ett effektivt sätt genomföra principerna för att skydda rättigheterna, hålla sig à jour med den senaste tekniken, ompröva risknivån osv. Behandlingarnas art, omfattning och sammanhang samt risken kan förändras under behandlingens gång, vilket innebär att den personuppgiftsansvarige kontinuerligt måste utvärdera sin behandling genom regelbundna översyner och bedömningar av effektiviteten hos de åtgärder och skyddsåtgärder som valts.

38. Skyldigheten att vid behov upprätthålla, se över och uppdatera behandlingen gäller även befintliga system. Det innebär att äldre system som utformades innan dataskyddsförordningen trädde i kraft måste ses över och underhållas för att säkerställa genomförandet av åtgärder och skyddsåtgärder som genomför de registrerades principer och rättigheter på ett effektivt sätt, i enlighet med dessa riktlinjer.

39. Denna skyldighet omfattar även all behandling som utförs med hjälp av personuppgiftsbiträden. De personuppgiftsansvariga ska regelbundet se över och utvärdera den behandling som utförs av personuppgiftsbiträden för att säkerställa kontinuerlig överensstämmelse med principerna och för att göra det möjligt för den personuppgiftsansvarige att fullgöra sina skyldigheter i detta avseende.

2.2 Artikel 25.2: Dataskydd som standard

2.2.1 Som standard behandlas endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen

40. En standard, såsom den vanligen definieras inom datavetenskapen, avser det befintliga eller förvalda värdet hos en konfigurerbar inställning som hänför sig till en programvarutillämpning, ett datorprogram eller en enhet. Sådana inställningar kallas även förinställningar eller fabriksinställningar, särskilt för elektroniska apparater.

41. Vid behandling av personuppgifter avser därför begreppet ”som standard” val av konfigurationsvärde eller behandlingsalternativ som fastställs eller föreskrivs i ett behandlingssystem, såsom en

programvara, tjänst eller enhet, eller ett manuellt behandlingsförfarande som påverkar mängden personuppgifter som samlas in, behandlingens omfattning, lagringstiden och deras tillgänglighet.

42. Den personuppgiftsansvarige bör välja och vara ansvarig för att införa standardinställningar och alternativ på ett sådant sätt att endast sådan behandling som är absolut nödvändig för att uppnå det fastställda, lagliga ändamålet utförs som standard. Här bör de personuppgiftsansvariga utgå från sin bedömning att behandlingen är nödvändig sett till de rättsliga grunderna i artikel 6.1. Detta innebär att den personuppgiftsansvarige som standard inte får samla in fler uppgifter än vad som är nödvändigt, inte får behandla de insamlade uppgifterna mer än vad som är nödvändigt för deras ändamål och inte heller får lagra uppgifterna längre än nödvändigt. Grundkravet är att dataskyddet ska vara inbyggt i den behandling som utförs som standard.

43. Den personuppgiftsansvarige ska i förväg bestämma för vilka särskilda, uttryckligt angivna och berättigade ändamål personuppgifterna ska samlas in och behandlas.[13] Åtgärderna ska som standard vara lämpliga för att säkerställa att endast personuppgifter som är nödvändiga för varje särskilt ändamål med behandlingen behandlas. Europeiska datatillsynsmannens riktlinjer för bedömning av om åtgärder som begränsar rätten till skydd av personuppgifter är nödvändiga och proportionerliga kan även vara användbara när det gäller att bestämma vilka uppgifter som det är nödvändigt att behandla för att uppnå ett särskilt syfte.[14] [15] [16]

44. Om den personuppgiftsansvarige använder tredjepartsprogram eller standardprogramvara bör den personuppgiftsansvarige utföra en riskbedömning av produkten och se till att funktioner som inte har någon rättslig grund eller som inte är kompatibla med de avsedda ändamålen med behandlingen stängs av.

45. Samma överväganden är tillämpliga på de organisatoriska åtgärder som stöder behandlingen. Dessa ska, redan från början, vara utformade så att endast den minsta mängd personuppgifter som krävs för de särskilda åtgärderna behandlas. Detta ska särskilt beaktas när personal med olika arbetsuppgifter och olika behov får åtkomst till uppgifter.

46. Lämpliga ”tekniska och organisatoriska åtgärder” i samband med dataskydd som standard ska således förstås på samma sätt som diskuteras ovan i avsnitt 2.1.1, men särskilt tillämpas på genomförandet av principen om uppgiftsminimering.

47. Ovannämnda skyldighet att enbart behandla personuppgifter som är nödvändiga för varje särskilt ändamål är tillämplig på följande omständigheter:

[13] Artikel 5.1 b, c, d och e i dataskyddsförordningen.

[14] Europeiska datatillsynsmannen. “Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection”. 25 februari 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] Se även Europeiska datatillsynsmannen. “Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit” https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

[16] För mer information om nödvändighet, se artikel 29-gruppens yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG. WP 217, 9 april 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_sv.pdf

2.2.2 Omfattningen av uppgiftsminimeringsskyldigheten

48. I artikel 25.2 anges omfattningen av uppgiftsminimeringsskyldigheten vid standardbehandling genom att det anges att skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet.

2.2.2.1 ”mängden insamlade personuppgifter”

49. Personuppgiftsansvariga bör beakta både mängden personuppgifter samt typerna, kategorierna och detaljnivån för de personuppgifter som krävs för ändamålet med behandlingen. Vid val av utformning ska de ta hänsyn till de ökade riskerna när det gäller principerna om säkerhet, uppgiftsminimering och lagringsminimering vid insamling av stora mängder detaljerade personuppgifter, och jämföra dem med de minskade riskerna vid insamling av mindre detaljerad information om de registrerade. Under alla omständigheter får standardinställningen inte omfatta insamling av personuppgifter som inte är nödvändiga för det särskilda ändamålet med behandlingen. Om vissa kategorier av personuppgifter är onödiga eller om det inte krävs några detaljerade uppgifter ska med andra ord eventuella överflödiga uppgifter inte samlas in, eftersom det är tillräckligt med mindre detaljerade uppgifter.

50. Samma standardkrav gäller för tjänster oberoende av vilken plattform eller enhet som används. Endast de personuppgifter som krävs för det aktuella ändamålet kan samlas in.

2.2.2.2 ”behandlingens omfattning”

51. Behandling[17] av personuppgifter ska begränsas till vad som är nödvändigt. Flera behandlingar kan behövas för att uppnå ändamålet med behandlingen. Att vissa personuppgifter är nödvändiga för att fullgöra ett ändamål betyder emellertid inte att alla typer av behandlingar får utföras eller att uppgifterna får behandlas hur ofta som helst. Personuppgiftsansvariga ska även vara försiktiga så att de inte utvidgar gränserna för förenliga ändamål i artikel 6.4, och ha i åtanke vilken behandling som täcks av de registrerades berättigade förväntningar.

2.2.2.3 ”tiden för deras lagring”

52. Personuppgifter som samlas in ska inte lagras om de inte är nödvändiga för ändamålet med behandlingen och det inte finns något annat förenligt ändamål och någon annan rättslig grund enligt artikel 6.4. Den personuppgiftsansvarige ska i enlighet med ansvarsprincipen objektivt motivera varför lagring är nödvändig.

53. Den personuppgiftsansvarige ska begränsa lagringstiden till vad som är nödvändigt för ändamålet. Om personuppgifter inte länge är nödvändiga för ändamålet med behandlingen ska de som standard raderas eller anonymiseras. Lagringstidens längd beror således på ändamålet med den aktuella behandlingen. Denna skyldighet har direkt samband med principen om lagringsminimering i artikel 5.1 e och ska genomföras som standard, dvs. den personuppgiftsansvarige bör ha systematiska förfaranden för radering av uppgifter eller anonymisering inbyggda i behandlingen.

[17] Enligt artikel 4.2 i dataskyddsförordningen omfattar detta 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.

54. Anonymisering[18] av personuppgifter är ett alternativ till radering, under förutsättning att alla relevanta omständigheter beaktas och riskens sannolikhetsgrad och allvar, inbegripet risken för avanonymisering, regelbundet utvärderas.[19]

2.2.2.4 ”deras tillgänglighet”

55. Den personuppgiftsansvarige bör begränsa vilka som kan få tillgång till personuppgifter (och vilken typ av tillgång) grundat på en bedömning av tillgångens nödvändighet, och även se till att personuppgifterna faktiskt är tillgängliga för dem som vid behov behöver dem, t.ex. i kritiska situationer. Åtkomstkontroller bör iakttas för hela dataflödet under behandlingen.

56. I artikel 25.2 anges vidare att personuppgifter – utan den enskildes medverkan – inte får göras tillgängliga för ett obegränsat antal fysiska personer. Den personuppgiftsansvarige ska som standard begränsa tillgängligheten och ge den registrerade möjlighet att ingripa innan dennes personuppgifter offentliggörs eller på annat sätt görs tillgängliga för ett obegränsat antal fysiska personer.

57. Om personuppgifter görs tillgängliga för ett obestämt antal personer kan detta leda till större spridning av uppgifterna än vad som ursprungligen avsågs. Detta är särskilt relevant i samband med internet och sökmotorer. Den personuppgiftsansvarige bör därför automatiskt ge registrerade möjlighet att ingripa innan personuppgifter görs tillgängliga på internet. Detta är särskilt viktigt när det gäller barn och utsatta grupper.

58. Beroende på de rättsliga grunderna för behandlingen kan möjligheten att ingripa variera beroende på behandlingens sammanhang. Det kan till exempel röra sig om att be om samtycke till att personuppgifterna görs allmänt tillgängliga eller att ha sekretessinställningar så att de registrerade själva kan kontrollera vem som har tillgång till uppgifterna.

59. Även om personuppgifter görs allmänt tillgängliga med den registrerades tillstånd och samtycke, innebär detta inte att alla andra personuppgiftsansvariga som har åtkomst till personuppgifterna själva har rätt att fritt behandla dem, för sina egna ändamål – de måste ha sin egen rättsliga grund.[20]

3 GENOMFÖRANDE AV PRINCIPERNA FÖR DATASKYDD VID BEHANDLING AV PERSONUPPGIFTER MED HJÄLP AV INBYGGT DATASKYDD OCH DATASKYDD SOM STANDARD

60. Den personuppgiftsansvarige bör i alla stadier av utformningen av behandlingen, inbegripet upphandling, anbud, utkontraktering, utveckling, support, underhåll, testning, lagring, radering osv.,

[18] Artikel 29-gruppen. Yttrande 05/2014 om avidentifieringsmetoder. WP 216, 10 april 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_sv.pdf.

[19] Se artikel 4.1 i dataskyddsförordningen, skäl 26 i dataskyddsförordningen och artikel 29-gruppens yttrande 05/2014 om avidentifieringsmetoder. Se även underavsnittet om lagringsminimering i avsnitt 3 i detta dokument, där det hänvisas till den personuppgiftsansvariges behov att säkerställa att den genomförda anonymiseringsmetoden är effektiv.

[20] Se mål nr 931/13, Satakunnan Markkinapörssi Oy och Satamedia Oy mot Finland.

ta hänsyn till och beakta de olika delarna av inbyggt dataskydd och dataskydd som standard som illustreras genom exempel i detta kapitel, i samband med genomförandet av dessa principer.[21] [22] [23]

61. Personuppgiftsansvariga måste genomföra principerna för att uppnå inbyggt dataskydd och dataskydd som standard. Dessa principer omfattar öppenhet, laglighet, rättvisa, ändamålsbegränsning, uppgiftsminimering, korrekthet, lagringsminimering, integritet och konfidentialitet samt ansvarsskyldighet. Principerna räknas upp i artikel 5 och i skäl 39 i dataskyddsförordningen. För att till fullo förstå hur dataskyddsförordningen ska genomföras är det viktigt att förstå innebörden av var och en av dessa principer.

62. I presentationen av exempel på hur inbyggt dataskydd och dataskydd som standard kan omsättas i praktiken har vi gjort en förteckning över **centrala komponenter i inbyggt dataskydd och dataskydd som standard** för var och en av principerna. Exemplen framhäver den aktuella dataskyddsprincipen, men kan även överlappa med andra närbesläktade principer. EDPB understryker att de centrala komponenterna och exemplen nedan varken är uttömmande eller bindande, utan är avsedda som vägledning för var och en av principerna. Personuppgiftsansvariga måste bedöma hur de kan garantera att principerna iakttas i samband med den konkreta behandlingen i fråga.

63. Även om detta avsnitt fokuserar på genomförandet av principerna bör den personuppgiftsansvarige även införa *lämpliga* och *effektiva* metoder för att skydda de registrerades rättigheter, även i enlighet med kapitel III i dataskyddsförordningen, om detta inte redan föreskrivs i själva principerna.

64. Principen om ansvarsskyldighet är en övergripande princip. Det innebär att den personuppgiftsansvarige ska vara ansvarig och välja nödvändiga tekniska och organisatoriska åtgärder.

3.1 Öppenhet[24]

65. Den personuppgiftsansvarige måste vara tydlig och öppen i sin kommunikation med den registrerade om hur personuppgifterna kommer att samlas in, användas och delas. Öppenhet handlar om att göra det möjligt för de registrerade att förstå och i förekommande fall använda sina rättigheter enligt artiklarna 15–22. Principen är inbyggd i artiklarna 12, 13, 14 och 34. Åtgärder och skyddsåtgärder som införts till stöd för principen om öppenhet ska även stödja genomförandet av dessa artiklar.

66. När det gäller öppenhetsprincipen kan följande betraktas som centrala komponenter i inbyggt dataskydd och dataskydd som standard:

- Klarhet: informationen ska vara på ett klart och tydligt språk, kortfattad och begriplig.
- Semantik: kommunikationen bör ha en tydlig innebörd för den aktuella publiken.
- Tillgänglighet: informationen ska vara lättillgänglig för den registrerade.
- Sammanhang: informationen bör tillhandahållas vid relevant tidpunkt och i lämplig form.
- Relevans: informationen bör vara relevant och tillämplig på den specifika registrerade personen.

[21] Fler exempel återfinns i den norska dataskyddsmyndighetens riktlinjer "Software Development with Data Protection by Design and by Default". 28 november 2017. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

[24] För en närmare utveckling av hur begreppet öppenhet ska tolkas, se artikel 29-gruppens riktlinjer om öppenhet enligt förordning (EU) 2016/679. WP 260 rev.01, 11 april 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 – godkända av EDPB.

- Allmän utformning: informationen ska vara tillgänglig för alla registrerade och omfatta användning av maskinläsbart språk för att underlätta och automatisera läsbarheten och klarheten.
- Begriplig: de registrerade bör kunna förstå vad de kan förvänta sig vad gäller behandlingen av deras personuppgifter, i synnerhet om de registrerade är barn eller tillhör andra utsatta grupper.
- Flera kanaler: informationen bör tillhandahållas via olika kanaler och medier, inte enbart skriftliga, för att öka sannolikheten att informationen når den registrerade på ett effektivt sätt.
- Skiktad: informationen bör skiktas på ett sätt som förenar behovet av fullständighet och behovet av förståelse, samtidigt som hänsyn tas till de registrerades rimliga förväntningar.

Exempel[25]

En personuppgiftsansvarig utformar en integritetspolicy på sin webbplats för att uppfylla kraven på öppenhet. Integritetspolicyn bör inte innehålla en stor mängd information som är svår för den genomsnittliga registrerade att tränga in i och förstå. Informationen ska vara klart och tydligt skriven och göra det lätt för webbplatsens användare att förstå hur deras personuppgifter behandlas. Den personuppgiftsansvarige tillhandahåller därför information på flera nivåer, där de viktigaste punkterna framhävs. Samtidigt är det lätt att få tillgång till mer detaljerad information. Rullmenyer och länkar till andra sidor tillhandahålls för att ytterligare förklara de olika poster och begrepp som används. Den personuppgiftsansvarige ser även till att informationen lämnas via flera kanaler och tillhandahåller videoklipp som förklarar de viktigaste punkterna i den skriftliga informationen. Synergieffekten mellan de olika sidorna är avgörande för att se till att den skiktade strategin inte ökar förvirringen, utan snarare minskar den.

Det ska vara enkelt för de registrerade att få tillgång till integritetspolicyn. Integritetspolicyn tillgänglig- och synliggörs således på alla webbsidor på den aktuella webbplatsen, så att den registrerade alltid bara är ett klick bort från att få tillgång till informationen. Den information som tillhandahålls utformas även enligt bästa praxis och standarder för allmän utformning så att den blir tillgänglig för alla.

Vidare bör den nödvändiga informationen tillhandahållas i rätt sammanhang och vid rätt tidpunkt. Eftersom den personuppgiftsansvarige utför många behandlingar med hjälp av de uppgifter som samlats in på webbplatsen räcker det inte med en allmän integritetspolicy enbart på webbplatsen för att den personuppgiftsansvarige ska kunna uppfylla kraven på öppenhet. Den personuppgiftsansvarige utformar därför ett informationsflöde som ger den registrerade relevant information i lämpliga sammanhang, t.ex. med hjälp av informativa notiser eller poppuppfönster. Till exempel ska den personuppgiftsansvarige, när denne ber den registrerade att ange sina personuppgifter, informera vederbörande om hur uppgifterna kommer att behandlas och varför dessa uppgifter är nödvändiga för behandlingen.

3.2 Laglighet

67. Den personuppgiftsansvarige ska identifiera en giltig rättslig grund för behandlingen av personuppgifterna. Åtgärder och skyddsåtgärder bör fungera som stöd för kravet på säkerställande av att hela behandlingens livscykel överensstämmer med de relevanta rättsliga grunderna för behandlingen.

[25] Den franska dataskyddsmyndigheten har offentliggjort flera exempel som illustrerar bästa praxis vad gäller information till användarna samt andra öppenhetsprinciper: https://design.cnil.fr/en/.

68. När det gäller laglighet kan följande betraktas som centrala komponenter i inbyggt dataskydd och dataskydd som standard:

- Relevans: korrekt rättslig grund ska tillämpas på behandlingen.
- Differentiering[26]: den rättsliga grund som används för varje behandlingsverksamhet ska differentieras.
- Specifikt ändamål: den lämpliga rättsliga grunden ska ha ett klart samband med det specifika ändamålet för behandlingen.[27]
- Nödvändighet: behandlingen ska vara nödvändig och ovillkorlig för att ändamålet ska vara lagligt.
- Autonomi: den registrerade ska ges så mycket autonomi som möjligt när det gäller kontrollen över personuppgifterna inom ramarna för den rättsliga grunden.
- Samtycke: samtycket måste vara frivilligt, specifikt, informerat och otvetydigt.[28] Barns och ungdomars förmåga att ge sitt informerade samtycke bör särskilt beaktas.
- Återkallande av samtycke: om samtycke utgör den rättsliga grunden bör behandlingen underlätta återkallandet av samtycket. Det ska vara lika enkelt att återkalla som att lämna samtycke. Om så inte är fallet är den personuppgiftsansvariges samtyckesmekanism inte förenlig med dataskyddsförordningen.[29]
- Intresseavvägning: om berättigade intressen utgör den rättsliga grunden måste den personuppgiftsansvarige göra en viktad avvägning mellan intressen, med särskild hänsyn till maktbalansen, särskilt när det gäller barn under 18 år och andra utsatta grupper. Det ska finnas åtgärder och skyddsåtgärder för att mildra de negativa konsekvenserna för de registrerade.
- Fastställande i förväg: den rättsliga grunden ska fastställas innan behandlingen äger rum.
- Upphörande: om en rättslig grund upphör att vara tillämplig ska även behandlingen upphöra.
- Justering: vid en giltig ändring av den rättsliga grunden för behandlingen ska den faktiska behandlingen justeras i enlighet med den nya rättsliga grunden.[30]
- Ansvarsfördelning: vid gemensamt ansvar krävs att parterna fördelar sitt respektive ansvar gentemot den registrerade på ett tydligt och öppet sätt, och utformar behandlingsåtgärderna i enlighet med denna fördelning.

Exempel

En bank planerar att erbjuda en tjänst för att förbättra effektiviteten vid hantering av låneansökningar. Idén bakom tjänsten är att banken, med kundens tillåtelse, kan inhämta uppgifter om kunden direkt från skattemyndigheterna. Detta exempel omfattar inte behandling av personuppgifter som härrör från andra källor.

[26] EDPB:s riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade, version 2.0, 8 oktober 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_sv.pdf

[27] Se avsnittet om ändamålsbegränsning nedan.

[28] Se ”Guidelines 05/2020 on consent under Regulation 2016/679”. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] Se ”Guidelines 05/2020 on consent under Regulation 2016/679”, s. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[30] Om den ursprungliga rättsliga grunden är samtycke, se ”Guidelines 05/2020 on consent under Regulation 2016/679”. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

Att inhämta personuppgifter om den registrerades ekonomiska situation är nödvändigt för att vidta åtgärder på den registrerades begäran innan ett låneavtal ingås.[31] Att samla in personuppgifter direkt från skatteförvaltningen anses dock inte nödvändigt, eftersom kunden kan ingå avtal genom att själv tillhandahålla denna information från skatteförvaltningen. Även om banken kan ha ett berättigat intresse av att få handlingarna direkt från skattemyndigheterna, till exempel för att säkerställa en effektiv lånehantering, utgör en sådan direkt tillgång till sökandes personuppgifter en risk i samband med användning eller eventuellt missbruk av åtkomsträttigheter.

Vid genomförandet av principen om laglighet inser den personuppgiftsansvarige att det i detta sammanhang inte går att använda grunden ”nödvändig för att fullgöra ett avtal” för den del av behandlingen som omfattar insamling av personuppgifter direkt från skattemyndigheterna. Det faktum att denna särskilda behandling medför en risk för att den registrerade blir mindre involverad i behandlingen av sina uppgifter är också en relevant omständighet i bedömningen av huruvida själva behandlingen är laglig. Banken drar slutsatsen att denna del av behandlingen måste bygga på en annan rättslig grund. I just den medlemsstat där den personuppgiftsansvarige är hemmahörande finns det nationella lagar som gör det möjligt för banken att direkt samla in information från skattemyndigheterna, om den registrerade i förväg har samtyckt till detta.

Banken lämnar därför information om behandlingen på den digitala ansökningsplattformen, på ett sätt som gör det enkelt för de registrerade att förstå vilken behandling som är obligatorisk och vilken som är frivillig. Behandlingsalternativen medger i standardfallet inte hämtning av uppgifter direkt från andra källor än den registrerade själv, och möjligheten till direkt inhämtning av information presenteras på ett sätt som inte hindrar den registrerade från att avstå. Ett eventuellt samtycke till att inhämta uppgifter direkt från andra personuppgiftsansvariga utgör en tillfällig rätt till tillgång till viss information.

Ett eventuellt samtycke behandlas elektroniskt på ett sätt som kan dokumenteras, och de registrerade kan enkelt kontrollera vad de har samtyckt till och återkalla sitt samtycke.

Den personuppgiftsansvarige har bedömt dessa villkor för inbyggt dataskydd och dataskydd som standard i förväg, och alla dessa kriterier har inkluderats i kravspecifikationen för anbudet att köpa in plattformen. Den personuppgiftsansvarige är medveten om att det antingen kan vara för sent att genomföra dataskyddet i efterhand, eller innebära ett mycket kostsamt förfarande, om villkoren för inbyggt dataskydd och dataskydd som standard inte inkluderas i kraven för anbudet.

3.3 Rättvisa

69. Rättvisa är en övergripande princip enligt vilken det krävs att personuppgifterna inte behandlas på ett sätt som är omotiverat missgynnande, olagligt diskriminerande, oväntat eller vilseledande för den registrerade. Åtgärder och skyddsåtgärder som genomför principen om rättvisa främjar även de registrerades rättigheter och friheter, särskilt rätten till information (öppenhet), rätten att ingripa (tillgång, radering, dataportabilitet och rättelse) och rätten att begränsa behandlingen (rätten att inte bli föremål för automatiserat individuellt beslutsfattande och icke-diskriminering av de registrerade i sådana förfaranden).

70. När det gäller rättvisa kan följande betraktas som centrala komponenter i inbyggt dataskydd och dataskydd som standard:

[31] Se artikel 6.1 b i dataskyddsförordningen.

- Autonomi: de registrerade bör ges största möjliga självbestämmande när det gäller att avgöra hur deras personuppgifter ska användas, samt i fråga om användningens eller behandlingens omfattning och villkor.
- Samspel: de registrerade måste kunna kommunicera med den personuppgiftsansvarige och utöva sina rättigheter i samband med de personuppgifter som denne behandlar.
- Förväntningar: behandlingen ska överensstämma med de registrerades rimliga förväntningar.
- Icke-diskriminering: den personuppgiftsansvarige får inte på ett orättvist sätt diskriminera de registrerade.
- Icke-utnyttjande: den personuppgiftsansvarige bör inte utnyttja de registrerades behov eller sårbarhet.
- Konsumenternas valfrihet: den personuppgiftsansvarige får inte ”låsa in” sina användare på ett orättvist sätt. När en tjänsts behandling av personuppgifter avser tjänstens egna uppgifter får den skapa en inlåsning till tjänsten. Om det försämrar de registrerades möjligheter att utöva sin rätt till dataportabilitet i enlighet med artikel 20 kan detta eventuellt betraktas som orättvist.
- Maktbalans: maktbalans bör vara ett centralt mål för förhållandet mellan den personuppgiftsansvarige och den registrerade. Maktobalanser bör undvikas. När detta inte går bör obalanser erkännas och åtgärdas med hjälp av lämpliga motåtgärder.
- Ingen risk för överföring: personuppgiftsansvariga bör inte överföra företagets risker på de registrerade.
- Inget bedrägeri: information och alternativ i samband med databehandling bör tillhandahållas på ett objektivt och neutralt sätt, så att man undviker bedrägligt eller manipulativt språk eller bedräglig eller manipulativ utformning.
- Respektera rättigheter: den personuppgiftsansvarige måste respektera de registrerades grundläggande rättigheter och vidta lämpliga åtgärder och skyddsåtgärder och får inte vidta åtgärder som inkräktar på dessa rättigheter, såvida detta inte uttryckligen motiveras i lag.
- Etiska aspekter: den personuppgiftsansvarige ska se behandlingens följdpåverkan på den enskildes rättigheter och värdighet.
- Sanningsenlighet: den personuppgiftsansvarige ska tillhandahålla information om hur de behandlar personuppgifter. De bör agera på det sätt som de har utlovat och inte vilseleda de registrerade.
- Mänsklig medverkan: den personuppgiftsansvarige måste införa krav på *kvalificerad* mänsklig medverkan för att upptäcka fel som maskiner kan skapa, i enlighet med rätten att inte bli föremål för ett automatiserat individuellt beslutsfattande i artikel 22.[32]
- Rättvisa algoritmer: den personuppgiftsansvarige ska regelbundet göra en bedömning av om algoritmerna fungerar i enlighet med syftena och justera algoritmerna för att rätta till systematiska fel (biaser) som upptäckts och säkerställa rättvis behandling. De registrerade bör informeras om hur den behandling av personuppgifter går till som grundas på algoritmer som analyserar eller gör förutsägelser om dem, såsom arbetsprestation, ekonomisk ställning, hälsa, personliga preferenser, tillförlitlighet eller beteende, vistelseort eller förflyttningar.[33]

[32] Se riktlinjerna om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[33] Se skäl 71 i dataskyddsförordningen.

Exempel 1

En personuppgiftsansvarig driver en sökmotor som behandlar personuppgifter som till övervägande del genererats av användarna. Den personuppgiftsansvarige drar fördel av att ha en stor mängd personuppgifter och kunna använda dessa personuppgifter för riktad reklam. Den personuppgiftsansvarige vill därför påverka de registrerade att lämna samtycke till mer omfattande insamling och användning av deras personuppgifter. Samtycke ska inhämtas genom att den registrerade informeras om på vilka olika sätt behandlingen kan genomföras.

Vid tillämpningen av principen om rättvisa, med beaktande av behandlingens art, omfattning, sammanhang och ändamål, inser den personuppgiftsansvarige att det inte är tillåtet att presentera alternativen på ett sätt som medför en påtryckning på den registrerade att tillåta den personuppgiftsansvarige att samla in fler personuppgifter än om alternativen skulle presenteras på ett likvärdigt och neutralt sätt. Detta innebär att den personuppgiftsansvarige inte kan presentera behandlingsalternativen på ett sätt som gör det svårt för de registrerade att avstå från att dela sina uppgifter, eller gör det svårt för dem att justera sina personliga inställningar och begränsa behandlingen. Detta är exempel på mörka mönster (så kallade *dark patterns*) som strider mot andan i artikel 25. Standardinställningarna för behandlingen bör inte vara för ingripande, och valet att tillåta ytterligare behandling bör presenteras på ett sätt som inte pressar den registrerade till att ge sitt samtycke. Därför presenterar den personuppgiftsansvarige valet mellan att ge eller inte ge samtycke som två likvärdiga alternativ, och återger på ett korrekt sätt vilka konsekvenser respektive val får för den registrerade.

Exempel 2

En annan personuppgiftsansvarig behandlar personuppgifter för tillhandahållande av en streamingtjänst där användarna kan välja mellan ett vanligt abonnemang med standardkvalitet och ett premiumabonnemang med högre kvalitet. Som en del av premiumabonnemanget får abonnenterna prioriterade kundtjänster.

Med beaktande av principen om rättvisa får de prioriterade kundtjänster som erbjuds premiumabonnenterna inte medföra att standardabonnenterna diskrimineras och inte ges samma möjligheter att utöva sina rättigheter enligt artikel 12 i dataskyddsförordningen. Detta innebär att även om premiumabonnenterna får prioriterade tjänster, får en sådan prioritering inte medföra en brist på lämpliga åtgärder för att besvara förfrågningar från standardabonnenter utan onödigt dröjsmål och senast inom en månad från det att förfrågningen gjordes.

Prioriterade kunder kan få betala för att erbjudas bättre tjänster, men alla registrerade ska ha likvärdig och icke-diskriminerande tillgång som gör det möjligt för dem att göra gällande sina rättigheter och friheter enligt artikel 12.

3.4 Ändamålsbegränsning[34]

[34] Artikel 29-gruppen har tillhandahållit vägledning för tolkningen av principen om ändamålsbegränsning enligt direktiv 95/46/EG. Även om yttrandet inte har antagits av EDPB kan det fortfarande vara relevant, eftersom principen har formulerats på samma sätt i dataskyddsförordningen. Artikel 29-gruppens yttrande 03/2013 om ändamålsbegränsning, WP 203, 2 april 2013, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

71. Den personuppgiftsansvarige måste samla in uppgifter för särskilda, uttryckligt angivna och berättigade ändamål och får inte senare behandla dem på ett sätt som är oförenligt med de ändamål för vilka de samlades in.[35] Behandlingen ska därför utformas med hänsyn till vad som är nödvändigt för att uppnå dessa syften. Om någon ytterligare behandling äger rum ska den personuppgiftsansvarige först säkerställa att ändamålen med denna behandling är förenliga med de ursprungliga ändamålen och utforma behandlingen på motsvarande sätt. Huruvida ett nytt ändamål är förenligt eller inte ska bedömas i enlighet med kriterierna i artikel 6.4.

72. När det gäller ändamålsbegränsning kan följande betraktas som centrala komponenter i inbyggt dataskydd och dataskydd som standard:
    - Fastställande i förväg: de berättigade ändamålen ska fastställas innan behandlingen utformas.
    - Specificitet: ändamålen ska specificeras, och det ska tydligt anges varför personuppgifterna behandlas.
    - Ändamålsorientering: behandlingens ändamål bör tjäna som vägledning för utformningen av behandlingen och fastställa gränser för den.
    - Nödvändighet: ändamålet avgör vilka personuppgifter som är nödvändiga för behandlingen.
    - Förenlighet: eventuella nya ändamål ska vara förenliga med det ursprungliga ändamål för vilket uppgifterna samlades in och tjäna som vägledning för relevanta ändringar av utformningen.
    - Begränsning av ytterligare behandling: den personuppgiftsansvarige får inte sammanföra uppsättningar av uppgifter eller genomföra någon ny behandling för nya, oförenliga ändamål.
    - Begränsningar för vidareutnyttjande: den personuppgiftsansvarige ska vidta tekniska åtgärder, inbegripet hashning och kryptering, för att begränsa möjligheten att använda personuppgifter för andra ändamål. Den personuppgiftsansvarige bör också se till att det finns organisatoriska åtgärder, såsom policyer och avtalsförpliktelser, som begränsar vidareutnyttjande av personuppgifter.
    - Översyn: den personuppgiftsansvarige bör regelbundet se över huruvida behandlingen är nödvändig för de ändamål för vilka uppgifterna samlades in och kontrollera att utformningen är förenlig med kravet på ändamålsbegränsning.

Exempel

Den personuppgiftsansvarige behandlar personuppgifter om sina kunder. Ändamålet med behandlingen är att fullgöra ett avtal, dvs. kunna leverera varor till rätt adress och erhålla betalning. De personuppgifter som lagras är köphistorik, namn, adress, e-postadress och telefonnummer.

Den personuppgiftsansvarige överväger att köpa en produkt för kundhantering som samlar alla kunduppgifter beträffande försäljning, marknadsföring och kundtjänst på ett och samma ställe. Produkten ger möjlighet att lagra alla telefonsamtal, åtgärder, dokument, e-postmeddelanden och marknadsföringskampanjer för att få en helhetsbild av kunden. Kundhanteringssystemet kan dessutom automatiskt analysera kundens köpkraft genom att använda offentlig information. Syftet med analysen är mer riktade reklamkampanjer. Detta är inte en del av det ursprungliga lagliga ändamålet för behandlingen.

För att kontrollera att kampanjerna är förenliga med principen om ändamålsbegränsning ger den personuppgiftsansvarige produktleverantören i uppdrag att kartlägga de olika behandlingarna där personuppgifter används för ändamål som är relevanta för den personuppgiftsansvarige.

[35] Artikel 5.1 b i dataskyddsförordningen.

Efter att ha mottagit resultaten av kartläggningen gör den personuppgiftsansvarige en bedömning av huruvida det nya marknadsföringssyftet och det riktade reklamsyftet är förenliga med de ursprungliga ändamål som fastställdes när uppgifterna samlades in, och om det finns en tillräcklig rättslig grund för respektive behandling. Om så inte är fallet ska den personuppgiftsansvarige sluta att använda respektive funktioner. Alternativt kan den personuppgiftsansvarige välja att avstå från bedömningen och helt enkelt inte använda produktens beskrivna funktioner.

3.5 Uppgiftsminimering

73. Endast personuppgifter som är adekvata, relevanta och **inte för omfattande** för ändamålet ska behandlas.[36] Mot denna bakgrund ska den personuppgiftsansvarige i förväg fastställa vilka funktioner och parametrar i behandlingssystemen och deras stödfunktioner som är tillåtna. Uppgiftsminimering underbygger och operationaliserar principen om nödvändighet. Vid den ytterligare behandlingen ska den personuppgiftsansvarige regelbundet bedöma om de personuppgifter som behandlats fortfarande är adekvata, relevanta och inte för omfattande, eller om uppgifterna ska raderas eller anonymiseras.

74. Personuppgiftsansvariga bör först fastställa om de över huvud taget behöver behandla personuppgifter för sina relevanta ändamål. Den personuppgiftsansvarige bör kontrollera om de relevanta ändamålen kan uppnås genom att behandla färre personuppgifter, ha mindre detaljerade eller sammanställda personuppgifter eller utan att behandla personuppgifter över huvud taget[37]. En sådan kontroll bör utföras före behandlingen, men kan också utföras när som helst under behandlingens livscykel. Detta är även förenligt med artikel 11.

75. Minimering kan också avse graden av identifiering. Om syftet med behandlingen inte kräver att den slutliga uppsättningen uppgifter hänför sig till en identifierad eller identifierbar enskild (såsom i statistik), men detta är fallet vid den inledande behandlingen (t.ex. före sammanställningen av uppgifterna), ska den personuppgiftsansvarige anonymisera uppgifterna så snart identifieringen inte längre är nödvändig. Om fortsatt identifiering emellertid behövs för en annan behandling ska personuppgifterna pseudonymiseras för att minska riskerna för de registrerades rättigheter.

76. När det gäller uppgiftsminimering kan följande betraktas som centrala komponenter i inbyggt dataskydd och dataskydd som standard:
    - Undvikande av data: behandling av personuppgifter ska undvikas helt när detta är möjligt för det relevanta ändamålet.
    - Begränsning: mängden personuppgifter som samlas in ska begränsas till vad som är nödvändigt för ändamålet.
    - Åtkomstbegränsning: uppgiftsbehandlingen bör utformas på ett sätt som innebär att ett minimalt antal personer behöver få åtkomst till personuppgifter för att kunna utföra sina arbetsuppgifter, och åtkomsten bör begränsas i överensstämmelse med detta.
    - Relevans: personuppgifter bör vara relevanta för den aktuella behandlingen, och den personuppgiftsansvarige bör kunna styrka denna relevans.
    - Nödvändighet: varje personuppgiftskategori ska vara nödvändig för de specifika ändamålen och får endast behandlas om det inte är möjligt att fullgöra ändamålet med andra medel.

[36] Artikel 5.1 c i dataskyddsförordningen.
[37] I skäl 39 i dataskyddsförordningen föreskrivs följande: ”… Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel.”

- Sammanställning: om möjligt ska sammanställda uppgifter användas.
- Pseudonymisering: personuppgifter ska pseudonymiseras så snart det inte längre är nödvändigt med direkt identifierbara personuppgifter och identifieringsnycklar ska lagras separat.
- Anonymisering och radering: om personuppgifterna inte, eller inte längre, är nödvändiga för ändamålet ska de anonymiseras eller raderas.
- Dataflöde: dataflödet bör göras tillräckligt effektivt för att inte skapa fler kopior än nödvändigt.
- Den senaste utvecklingen: den personuppgiftsansvarige ska tillämpa tillgänglig och lämplig teknik för undvikande av data och uppgiftsminimering.

Exempel 1

En bokhandel vill öka sina intäkter genom att sälja böcker på nätet. Ägaren vill upprätta ett standardiserat beställningsformulär. För att se till att kunderna fyller i all nödvändig information gör ägaren alla fält i formuläret obligatoriska (om de inte fylls i kan kunden inte göra någon beställning). Ägaren använder inledningsvis ett standardiserat formulär för kontaktuppgifter, där bland annat kundens födelsedatum, telefonnummer och hemadress efterfrågas. Alla fält i formuläret är emellertid inte nödvändiga för ändamålet att köpa och leverera böcker. Om den registrerade betalar för produkten i förskott är den registrerades födelsedatum och telefonnummer inte nödvändiga för inköpet av produkten. Detta innebär att dessa fält inte får vara obligatoriska i webbformuläret för att beställa produkten, såvida inte den personuppgiftsansvarige tydligt kan visa att detta är nödvändigt och varför. Vidare finns det situationer där det inte krävs någon adress. När kunden beställer en e-bok kan han eller hon till exempel ladda ner produkten direkt till sin enhet.

Ägaren till webbshopen beslutar därför att göra två webbformulär, ett för att beställa böcker, med ett fält för kundens adress, och ett webbformulär för att beställa e-böcker utan något fält för kundens adress.

Exempel 2

Ett kollektivtrafikföretag vill samla in statistiska uppgifter på grundval av passagerarnas resvägar. Detta är användbart för ändamålet att göra rätt val vad gäller ändringar av tidtabeller och fastställande av tågsträckor. Passagerarna måste dra sina biljetter genom en läsapparat varje gång de stiger på eller av ett transportmedel. Efter att ha genomfört en riskbedömning avseende passagerarnas rättigheter och friheter i samband med insamling av uppgifter om deras resvägar, slår den personuppgiftsansvarige fast att det är möjligt att utifrån en enda resvägsidentifiering identifiera passagerare med hjälp av biljettens identifieringskod, om dessa bor eller arbetar i glesbefolkade områden. Av detta skäl lagrar inte den personuppgiftsansvarige biljettens identifieringskod, eftersom det inte är nödvändigt för ändamålet att optimera tidtabellerna och tågsträckorna. När resan väl är avslutad lagrar den personuppgiftsansvarige endast de individuella resvägarna, för att resor som är knutna till en enskild biljett inte ska kunna identifieras, och sparar endast information som hänför sig till separata resvägar.

I situationer där det fortfarande kan finnas en risk för att en person identifieras enbart genom sin kollektivtrafikresväg vidtar den personuppgiftsansvarige åtgärder för att minska risken, t.ex. tar bort början och slutet på resan.

Exempel 3

En budfirma har för avsikt att bedöma hur effektiva dess leveranser är vad gäller leveranstider, planering av arbetsbelastningen och bränsleförbrukning. För att nå detta mål måste budfirman behandla ett antal personuppgifter som både hänför sig till anställda (chaufförer) och kunder (adresser, artiklar som ska levereras etc.). Denna behandling medför risker både för övervakning av anställda, vilket kräver särskilda rättsliga skyddsåtgärder, och spårning av kundernas vanor genom kunskap om levererade artiklar över tid. Dessa risker kan minskas avsevärt genom lämplig pseudonymisering av anställda och kunder. Effektiv uppgiftsminimering uppnås i synnerhet om pseudonymiseringskoder byts ut ofta och större områden beaktas i stället för exakta adresser, och den personuppgiftsansvarige kan fokusera enbart på leveransprocessen och på syftet resursoptimering, utan att överskrida tröskeln för övervakning av enskildas (kunders eller anställdas) beteenden.

Exempel 4

Ett sjukhus samlar in uppgifter om sina patienter i ett sjukhusinformationssystem (elektronisk patientjournal). Sjukhuspersonalen måste få åtkomst till patientjournaler för att kunna fatta beslut om vård och behandling av patienterna och för att dokumentera alla diagnos-, vård- och behandlingsåtgärder som vidtagits. Som standard beviljas åtkomst endast till den medicinska personal som behandlar respektive patient på den specialavdelning som han eller hon arbetar vid. Gruppen av personer med åtkomst till patientjournalen utökas om andra avdelningar eller diagnosenheter deltar i behandlingen. Efter det att patienten har skrivits ut och fakturerats begränsas åtkomsten till en liten grupp anställda per specialavdelning, vilka besvarar förfrågningar om medicinsk information eller en konsultation som görs eller efterfrågas av andra vårdgivare med respektive patients tillstånd.

3.6 Korrekthet

77. Personuppgifter ska vara korrekta och 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.[38]

78. Kraven bör betraktas i förhållande till de risker och konsekvenser som den konkreta användningen av uppgifter kan medföra. Felaktiga personuppgifter kan utgöra en risk för de registrerades rättigheter och friheter, t.ex. om det leder till en felaktig diagnos eller en felaktig behandling av en journal, och en felaktig bild av en person kan leda till att beslut fattas på felaktiga grunder, antingen manuellt, med användning av automatiserat beslutsfattande eller genom artificiell intelligens.

79. När det gäller korrekthet kan följande betraktas som centrala komponenter i inbyggt dataskydd och dataskydd som standard:
    - Datakälla: källor till personuppgifter bör vara tillförlitliga i den meningen att uppgifterna är korrekta.
    - Noggrannhet: varje del av personuppgifterna bör vara så korrekt som krävs för de specifika ändamålen.

[38] Artikel 5.1 d i dataskyddsförordningen.

- Mätbar korrekthet: minska antalet falska positiva/negativa resultat, t.ex. systematiska fel i automatiserade beslut och artificiell intelligens.
- Kontroll: den personuppgiftsansvarige ska, beroende på uppgifternas art, i förhållande till hur ofta de kan förändras, tillsammans med den registrerade före och efter olika steg i behandlingen kontrollera huruvida personuppgifterna är korrekta (t.ex. när det gäller ålderskrav).
- Radering/rättelse: den personuppgiftsansvarige ska radera eller rätta felaktiga uppgifter utan dröjsmål. Den personuppgiftsansvarige ska i synnerhet underlätta dessa åtgärder om de registrerade är eller var barn och senare vill ta bort sådana personuppgifter.[39]
- Undvikande av felfortplantning: personuppgiftsansvariga bör minska effekterna av ett ackumulerat fel i behandlingskedjan.
- Tillgång: de registrerade bör få information om och faktisk tillgång till personuppgifter i enlighet med artiklarna 12–15 i dataskyddsförordningen för att kontrollera att uppgifterna är korrekta och vid behov korrigera dem.
- Fortsatt korrekthet: personuppgifter ska vara korrekta i alla skeden av behandlingen och kontroller av korrektheten ska utföras vid kritiska steg.
- Uppdatering: personuppgifter ska om nödvändigt vara uppdaterade för ändamålet.
- Datautformning: användning av tekniska och organisatoriska konstruktionsegenskaper för att minska oklarheter, till exempel korta och förutbestämda val i stället för fritextfält.

Exempel 1

Ett försäkringsbolag vill använda artificiell intelligens (AI) för att göra en profilering av kunder som köper försäkringar och låta denna ligga till grund för sina beslut i samband med beräkningen av försäkringsrisken. När bolaget bestämmer hur AI-lösningarna ska utformas fastställer det hur behandlingen ska gå till och måste därför överväga inbyggt dataskydd när den väljer en AI-applikation från en säljare, och när den bestämmer hur lösningarna ska programmeras.

Den personuppgiftsansvarige bör ha korrekta uppgifter när denne bestämmer hur AI-lösningarna ska programmeras, så att exakta resultat kan uppnås. Den personuppgiftsansvarige bör därför säkerställa att de uppgifter som används för att programmera lösningarna är korrekta.

Under förutsättning att den personuppgiftsansvarige har en rättslig grund för att programmera AI-lösningarna med hjälp av personuppgifter från en stor delgrupp befintliga kunder, väljer den personuppgiftsansvarige ut en kundgrupp som är representativ för populationen för att undvika systematiska fel.

Kunduppgifterna samlas sedan in från respektive datahanteringssystem, inklusive uppgifter om typen av försäkring, t.ex. sjukförsäkring, hemförsäkring och reseförsäkring, samt uppgifter från offentliga register som de har laglig tillgång till. Alla uppgifter pseudonymiseras innan de överförs till det system som är tänkt att lära upp AI-modellen.

För att säkerställa att uppgifterna som används för att programmera AI-lösningarna är så korrekta som möjligt samlar den personuppgiftsansvarige endast in uppgifter från datakällor med korrekt och uppdaterad information.

Försäkringsbolaget prövar om AI-systemet är tillförlitligt och ger icke-diskriminerande resultat, både under utvecklingsfasen och innan produkten släpps ut på marknaden. När AI-systemet är fullupplärt och operativt använder försäkringsbolaget resultaten som stöd för sina riskbedömningar av olika

[39] Se skäl 65.

försäkringar. Det förlitar sig dock inte enbart på AI för sitt beslut om beviljande av en försäkring, såvida inte beslutet fattas i enlighet med undantagen i artikel 22.2 i dataskyddsförordningen.

Försäkringsbolaget ser dessutom regelbundet över AI-resultaten för att upprätthålla tillförlitligheten och justerar vid behov algoritmen.

Exempel 2

Den personuppgiftsansvarige är en hälso- och sjukvårdsinrättning som söker efter metoder för att säkerställa integriteten och korrektheten hos personuppgifter i sina kundregister.

I situationer där två personer samtidigt kommer dit och får samma behandling finns det en förväxlingsrisk om deras namn är det enda kriteriet för att skilja dem åt. För att säkerställa korrektheten behöver den personuppgiftsansvarige en unik identifieringsbeteckning för varje person, och därmed mer information än enbart patientens namn.

Hälso- och sjukvårdsinrättningen använder flera system som innehåller personlig information om patienter och behöver se till att den information som hänför sig till patienten är korrekt, tillförlitlig och konsekvent i alla system vid alla tidpunkter. Den har identifierat flera risker som kan uppkomma om informationen ändras i ett system men inte i ett annat.

Den personuppgiftsansvarige beslutar att minska risken med hjälp av en hashningsteknik som kan användas för att säkerställa integriteten hos uppgifterna i patientjournalerna. Oföränderliga krypterade tidsstämplar skapas för patientjournalerna och den patient med vilken de är förknippade, så att eventuella ändringar kan upptäckas, tolkas och vid behov spåras.

3.7 Lagringsminimering

80. Den personuppgiftsansvarige ska säkerställa att personuppgifter lagras i ett format som inte gör det möjligt att identifiera de registrerade längre än nödvändigt för de ändamål för vilka personuppgifterna behandlas.[40]
Det är avgörande att den personuppgiftsansvarige vet exakt vilka personuppgifter som företaget behandlar och varför. Ändamålet med behandlingen ska vara huvudkriteriet för hur länge personuppgifterna ska lagras.

81. Åtgärder och skyddsåtgärder för att genomföra principen om lagringsminimering ska komplettera de registrerades rättigheter och friheter, särskilt rätten till radering och rätten att göra invändningar.

82. När det gäller lagringsminimering kan följande betraktas som centrala komponenter i inbyggt dataskydd och dataskydd som standard:
    - Radering och anonymisering: den personuppgiftsansvarige bör ha tydliga interna förfaranden och funktioner för radering och/eller anonymisering.
    - Effektiviteten hos anonymisering/radering: den personuppgiftsansvarige ska se till att det inte är möjligt att återidentifiera anonymiserade uppgifter, eller återskapa raderade uppgifter, och bör kontrollera om detta är möjligt.
    - Automatisering: raderingen av vissa personuppgifter bör automatiseras.

[40] Artikel 5.1 c i dataskyddsförordningen.

- Lagringskriterier: den personuppgiftsansvarige ska bestämma vilka uppgifter som är nödvändiga och vilken lagringsperiod som är nödvändig för ändamålet.
- Motivering: den personuppgiftsansvarige ska kunna motivera varför lagringsperioden är nödvändig för ändamålet och personuppgifterna i fråga och kunna redogöra för skälen till och de rättsliga grunderna för lagringsperioden.
- Genomförande av lagringsstrategier: den personuppgiftsansvarige bör införa interna lagringsstrategier och kontrollera om organisationen tillämpar strategierna.
- Säkerhetskopior/loggar: personuppgiftsansvariga ska bestämma vilka personuppgifter och vilken lagringstid som behövs för säkerhetskopior och loggar.
- Dataflöde: personuppgiftsansvariga bör vara vaksamma i fråga om flödet av personuppgifter och lagringen av eventuella kopior av uppgifterna och försöka begränsa ”tillfällig” lagring av dessa.

Exempel

Den personuppgiftsansvarige samlar in personuppgifter där syftet med behandlingen är att administrera ett medlemskap som den registrerade har. Personuppgifterna ska raderas när medlemskapet avslutas och det inte finns någon rättslig grund för ytterligare lagring av uppgifterna.

Den personuppgiftsansvarige utarbetar först ett internt förfarande för lagring och radering av uppgifter. Enligt detta förfarande ska de anställda radera personuppgifterna manuellt när lagringsperioden löper ut. Den anställde följer förfarandet för att regelbundet radera och rätta uppgifter från alla enheter, från säkerhetskopior, loggar, e-postmeddelanden och andra relevanta lagringsmedier.

För att raderingen ska bli mer effektiv och mindre felbenägen inför den personuppgiftsansvarige sedan i stället ett automatiskt system, så att uppgifter kan raderas automatiskt på ett tillförlitligt och mer regelbundet sätt. Systemet är konfigurerat att följa det föreskrivna förfarandet för radering av uppgifter, vilket sedan sker med i förväg fastställda, regelbundna intervall för att avlägsna personuppgifter från alla företagets lagringsmedier. Den personuppgiftsansvarige ser regelbundet över och testar lagringsförfarandet och säkerställer att det överensstämmer med aktuell lagringspolicy.

3.8 Integritet och konfidentialitet

83. Principen om integritet och konfidentialitet omfattar skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med hjälp av lämpliga tekniska eller organisatoriska åtgärder. Säkerheten i samband med personuppgifter kräver lämpliga åtgärder som utformats för att förhindra och hantera personuppgiftsincidenter, för att garantera att behandlingen av uppgifterna utförs på ett korrekt sätt och att de övriga principerna iakttas, samt för att underlätta för personer att utöva sina rättigheter.

84. I skäl 78 anges att en åtgärd för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard kan vara att den personuppgiftsansvarige får möjlighet att *”skapa och förbättra säkerhetsanordningar”.* Tillsammans med andra åtgärder avseende inbyggt dataskydd och dataskydd som standard visar skäl 78 att personuppgiftsansvariga har ett ansvar för att kontinuerligt utvärdera huruvida de använder lämpliga medel för behandlingen, och huruvida de åtgärder som valts faktiskt motverkar den befintliga sårbarheten. Personuppgiftsansvariga bör dessutom regelbundet se över de

åtgärder för informationssäkerhet som omgärdar och skyddar personuppgifterna och förfarandet för hantering av personuppgiftsincidenter.

85. När det gäller integritet och konfidentialitet kan följande betraktas som centrala komponenter i inbyggt dataskydd och dataskydd som standard:

- System för hantering av informationssäkerhet: ha ett operativt medel för hantering av strategier och förfaranden för informationssäkerhet.
- Riskanalys: bedömning av säkerhetsriskerna i samband med personuppgifter genom att beakta riskernas inverkan på enskildas rättigheter och motverka identifierade risker. Inom ramen för riskbedömningen utveckla och upprätthålla en omfattande, systematisk och realistisk ”hotmodellering” och en analys av angreppsytan av den programvara som utformats för att minska angreppsvektorer och möjligheter att utnyttja svaga punkter och sårbarheter.
- Inbyggd säkerhet: beakta säkerhetskraven så tidigt som möjligt i utformningen och utvecklingen av systemet och kontinuerligt integrera och utföra relevanta tester.
- Underhåll: regelbunden översyn och testning av programvara, maskinvara, system och tjänster osv. för att upptäcka sårbarheter hos de system som stöder behandlingen.
- Åtkomstkontroll: endast den behöriga personal som behöver bör ha tillgång till de personuppgifter som krävs för behandlingen, och den personuppgiftsansvarige bör skilja mellan behörig personals åtkomsträttigheter.
    - Åtkomstbegränsning (ombud): utforma uppgiftsbehandlingen på ett sätt som innebär att ett minimalt antal personer behöver få åtkomst till personuppgifter för att kunna utföra sina arbetsuppgifter, och begränsa åtkomsten i överensstämmelse med detta.
    - Åtkomstbegränsning (innehåll): i samband med varje behandling begränsa åtkomsten till endast de attribut per datamängd som behövs för att utföra den behandlingen. Dessutom begränsa åtkomsten till uppgifter som rör de registrerade som omfattas av respektive anställds ansvarsområde.
    - Åtkomstsegregering: utforma uppgiftsbehandlingen på ett sådant sätt som innebär att ingen enskild person behöver få omfattande tillgång till alla uppgifter som samlats in om en registrerad person, och än mindre alla personuppgifter för en viss kategori av registrerade.
- Säkra överföringar: överföringar ska vara säkrade mot obehörig och oavsiktlig åtkomst och ändringar.
- Säker lagring: lagringen av uppgifter ska vara säkrad mot obehörig åtkomst och ändringar. Det bör finnas förfaranden för att bedöma risken för centraliserad eller decentraliserad lagring och vilka kategorier av personuppgifter som omfattas av sådan lagring. Vissa uppgifter kan behöva mer säkerhetsåtgärder än andra, eller behöva isoleras från andra uppgifter.
- Pseudonymisering: personuppgifter och säkerhetskopior/loggar ska pseudonymiseras som en säkerhetsåtgärd för att minimera riskerna för eventuella personuppgiftsincidenter, t.ex. med hjälp av hashning eller kryptering.
- Säkerhetskopior/loggar: lagra säkerhetskopior och loggar i den utsträckning som behövs för informationssäkerheten, använd verifieringskedjor och övervakning av händelser som en rutinmässig säkerhetskontroll. Dessa ska skyddas mot obehörig och oavsiktlig åtkomst och ändring och regelbundet ses över. Incidenter bör hanteras omgående.
- Katastrofåterställning/driftskontinuitet: hantera krav på katastrofåterställning av informationssystem och driftskontinuitetskrav för att återställa tillgången till personuppgifter efter större incidenter.

- Skydd i enlighet med risk: alla kategorier av personuppgifter bör skyddas med lämpliga åtgärder med avseende på risken för säkerhetsincidenter. Uppgifter som utgör särskilda risker bör om möjligt hållas åtskilda från övriga personuppgifter.
- Incidenthanteringsförvaltning: ha rutiner, förfaranden och resurser för att upptäcka, begränsa, hantera, rapportera och lära av personuppgiftsincidenter.
- Incidenthantering: den personuppgiftsansvarige bör ha rutiner för att hantera överträdelser och incidenter, i syfte att göra behandlingssystemet mer robust. Detta inbegriper anmälningsförfaranden, såsom hantering av anmälningar (till tillsynsmyndigheten) och information (till de registrerade).

Exempel

En personuppgiftsansvarig vill extrahera stora mängder personuppgifter från en medicinsk databas som innehåller elektroniska patientjournaler till en särskild databasserver i företaget för att behandla de insamlade uppgifterna i kvalitetssäkringssyfte. Företaget har gjort bedömningen att en dirigering av dessa utdrag till en server som är tillgänglig för alla företagets anställda sannolikt medför en hög risk för de registrerades rättigheter och friheter. Eftersom det bara finns en avdelning i företaget som verkligen behöver behandla utdragen ur patientjournalerna beslutar den personuppgiftsansvarige att begränsa tillgången till den särskilda servern till anställda vid den avdelningen. För att ytterligare minska risken pseudonymiseras dessutom uppgifterna innan de överförs.

För att reglera åtkomsten och minska eventuella skador från sabotageprogram beslutar företaget att avskilja nätverket och införa åtkomstkontroller till servern. Dessutom inför företaget säkerhetsövervakning och ett system för förebyggande och detektering av intrång, som åtskiljs från rutinanvändningen. Ett automatiskt revisionssystem inrättas för att övervaka åtkomst och ändringar. Detta generar rapporter och automatiska varningar när vissa händelser med anknytning till användning konfigureras. Den personuppgiftsansvarige säkerställer att alla användare endast har åtkomst i förhållande till sina behov och med lämplig behörighetsnivå. Otillbörlig användning kan upptäckas snabbt och enkelt.

Vissa av utdragen behöver jämföras med nya utdrag och måste därför lagras i tre månader. Den personuppgiftsansvarige beslutar att placera dem i separata databaser på samma server och använder både transparent kryptering och kryptering på kolumnnivå för att lagra dem. Nycklar för dekryptering av kolumndata lagras i särskilda säkerhetsmoduler som endast kan användas av behörig personal, men inte extraheras.

Hanteringen av kommande incidenter gör systemet mer robust och tillförlitligt. Den personuppgiftsansvarige inser att förebyggande och effektiva åtgärder och skyddsåtgärder bör byggas in i all dess aktuella och framtida behandling av personuppgifter, och att detta bidrar till att förhindra personuppgiftsincidenter i framtiden.

Den personuppgiftsansvarige vidtar dessa säkerhetsåtgärder både för att säkerställa korrekthet, integritet och konfidentialitet, men även för att motverka spridning av sabotageprogram genom it-attacker och för att göra lösningen robust. Robusta säkerhetsåtgärder bidrar till att öka de registrerades förtroende.

3.9 Ansvarsskyldighet[41]

86. Enligt principen om ansvarsskyldighet ska den personuppgiftsansvarige ansvara för och kunna visa att alla ovannämnda principer följs.

87. Den personuppgiftsansvarige måste kunna visa att principerna följs. I samband med detta får den personuppgiftsansvarige visa effekterna av de åtgärder som vidtagits för att skydda de registrerades rättigheter och varför åtgärderna anses vara lämpliga och effektiva. Det kan till exempel handla om att visa varför en åtgärd är lämplig för att säkerställa principen om lagringsminimering på ett effektivt sätt.

88. För att kunna behandla personuppgifter på ett ansvarsfullt sätt bör den personuppgiftsansvarige ha både kunskap om och förmåga att genomföra dataskydd. Detta innebär att den personuppgiftsansvarige bör förstå sina dataskyddsskyldigheter enligt dataskyddsförordningen och kunna fullgöra dessa skyldigheter.

4 ARTIKEL 25.3 CERTIFIERING

89. Enligt artikel 25.3 får certifiering i enlighet med artikel 42 användas för att visa att kravet på inbyggt dataskydd och dataskydd som standard följs. Omvänt kan dokument som visar att kravet på inbyggt dataskydd och dataskydd som standard följs också vara användbara i en certifieringsprocess. Detta innebär att om en behandling som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde har certifierats i enlighet med artikel 42 ska tillsynsmyndigheten beakta detta vid sin bedömning av huruvida dataskyddsförordningen har följts, särskilt med avseende på inbyggt dataskydd och dataskydd som standard.

90. När en behandling som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde certifieras i enlighet med artikel 42 är de faktorer som bidrar till att visa att artikel 25.1 och 25.2 har följts de processer som har använts för att utforma skyddet, dvs. processen för att fastställa behandlingsmetoder, styrning och tekniska och organisatoriska åtgärder för att genomföra principerna för dataskydd. Kriterierna för certifiering av dataskydd fastställs av certifieringsorganen eller ägarna av certifieringssystemet och godkänns därefter av den behöriga tillsynsmyndigheten eller av EDPB. För ytterligare information om certifieringsmekanismer hänvisas läsaren till EDPB:s riktlinjer om certifiering[42] och annan relevant vägledning, som offentliggjorts på EDPB:s webbplats.

91. Även om en behandling har certifierats i enlighet med artikel 42 har den personuppgiftsansvarige fortfarande ansvaret för att kontinuerligt övervaka och förbättra efterlevnaden av kriterierna för inbyggt dataskydd och dataskydd som standard i artikel 25.

5 VERKSTÄLLIGHET AV ARTIKEL 25 OCH DESS KONSEKVENSER

92. Tillsynsmyndigheterna kan bedöma överensstämmelse med artikel 25 i enlighet med de förfaranden som anges i artikel 58. De korrigerande befogenheterna anges i artikel 58.2 och omfattar utfärdande av varningar, reprimander, föreläggande att tillmötesgå den registrerades rättigheter, begränsningar av eller förbud mot behandling, administrativa sanktionsavgifter m.m.

[41] Se skäl 74, enligt vilket personuppgiftsansvariga är skyldiga att visa att deras åtgärder är effektiva.
[42] EDPB. Riktlinjer 1/2018 om certifiering och fastställande av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordningen. Version 3.0, 4 juni 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_sv.pdf

93. Inbyggt dataskydd och dataskydd som standard är dessutom en faktor vid fastställande av ekonomiska sanktioner för åsidosättande av dataskyddsförordningen, se artikel 83.4.[43] [44]

6 REKOMMENDATIONER

94. Även om personuppgiftsbiträden och producenter inte uttryckligen nämns i artikel 25 erkänns även de som viktiga för att möjliggöra inbyggt dataskydd och dataskydd som standard, och de bör därför vara medvetna om att personuppgiftsansvariga endast behöver behandla personuppgifter med system och teknik som har inbyggt uppgiftsskydd.

95. Vid behandling för personuppgiftsansvarigas räkning, eller vid tillhandahållande av lösningar till personuppgiftsansvariga, bör personuppgiftsbiträden och producenter utnyttja sina expertkunskaper för att bygga upp förtroende och vägleda sina kunder, inbegripet små och medelstora företag, vid utformning/upphandling av lösningar som integrerar dataskydd i behandlingen. Detta innebär i sin tur att utformningen av produkter och tjänster bör underlätta de personuppgiftsansvarigas behov.

96. Vid genomförande av artikel 25 bör man tänka på att den främsta målsättningen med utformningen är att föra in ett *effektivt genomförande* av principerna och *skydd* av de registrerades rättigheter i de lämpliga åtgärderna i samband med behandlingen. För att underlätta och förbättra införandet av inbyggt dataskydd och dataskydd som standard lämnar vi följande rekommendationer till personuppgiftsansvariga, producenter och personuppgiftsbiträden:
    - Personuppgiftsansvariga bör tänka på inbyggt dataskydd och dataskydd som standard från de *inledande planeringsstadierna* av en behandling, till och med innan det fastställs vilka medel som ska användas för behandlingen.
    - Om den personuppgiftsansvarige har ett dataskyddsombud uppmuntrar EDPB dataskyddsombudet att aktivt medverka för att integrera inbyggt dataskydd och dataskydd som standard i upphandlings- och utvecklingsförfarandena samt i hela behandlingens livscykel.
    - En behandling kan vara *certifierad*. Möjligheten att få en behandling certifierad tillför ett mervärde för en personuppgiftsansvarig när han eller hon väljer mellan olika typer av programvara, maskinvara, tjänster och/eller system från producenter eller personuppgiftsbiträden. Producenterna bör därför sträva efter att visa att de har inbyggt dataskydd och dataskydd som standard i livscykeln för deras utveckling av en behandlingslösning. Ett certifieringssigill kan också vägleda registrerade i deras val mellan olika varor och tjänster. Möjligheten att få en behandling certifierad kan vara en konkurrensfördel för producenter, personuppgiftsbiträden och personuppgiftsansvariga, och ökar till och med de registrerades förtroende för behandlingen av deras personuppgifter. Om ingen certifiering erbjuds ska de personuppgiftsansvariga försöks få andra *garantier* för att producenter och personuppgiftsbiträden uppfyller kraven på inbyggt dataskydd och dataskydd som standard.

[43] I artikel 83.2 d i dataskyddsförordningen föreskrivs att vid påförande av sanktionsavgifter för åsidosättande av nämnda förordning ska ”vederbörlig hänsyn” tas till *”[g]raden av ansvar hos den personuppgiftsansvarige eller personuppgiftsbiträdet med beaktande av de tekniska och organisatoriska åtgärder som genomförts av dem i enlighet med artiklarna 25 och 32”*.

[44] Mer information om sanktionsavgifter återfinns i artikel 29-gruppens riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679, WP 253, 3 oktober 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 – godkända av EDPB.

- Personuppgiftsansvariga, personuppgiftsbiträden och producenter bör överväga sina skyldigheter att ge barn under 18 år och andra utsatta grupper särskilt skydd när de uppfyller kraven på inbyggt dataskydd och dataskydd som standard.
- Producenter och personuppgiftsbiträden bör sträva efter att underlätta genomförandet av inbyggt dataskydd och dataskydd som standard för att stödja den personuppgiftsansvariges förmåga att fullgöra skyldigheterna enligt artikel 25. Personuppgiftsansvariga bör däremot inte välja producenter och personuppgiftsbiträden som inte erbjuder system som gör det möjligt för den personuppgiftsansvarige att iaktta kraven i artikel 25, eftersom de kommer att hållas ansvariga för bristande genomförande av artikeln.
- Producenter och personuppgiftsbiträden bör spela en aktiv roll för att säkerställa att kraven när det gäller den senaste utvecklingen är uppfyllda, och underrätta de personuppgiftsansvariga om eventuella ändringar av den senaste utvecklingen som kan påverka effektiviteten hos de åtgärder som har införts. De personuppgiftsansvariga bör införa detta krav som en avtalsklausul för att säkerställa att de hålls uppdaterade.
- EDPB rekommenderar personuppgiftsansvariga att kräva att producenter och personuppgiftsbiträden visar hur deras maskinvara, programvara, tjänster eller system gör det möjligt för den personuppgiftsansvarige att uppfylla kraven på ansvarsskyldighet i enlighet med inbyggt dataskydd och dataskydd som standard, till exempel genom att använda nyckelutförandeindikatorer för att visa hur effektiva åtgärderna och skyddsåtgärderna är när det gäller att genomföra principerna och rättigheterna.
- EDPB framhåller behovet av ett harmoniserat tillvägagångssätt för att genomföra principer och rättigheter på ett effektivt sätt och uppmuntrar även sammanslutningar eller organ som utarbetar uppförandekoder enligt artikel 40 att införliva sektorspecifik vägledning om inbyggt dataskydd och dataskydd som standard.
- De personuppgiftsansvariga bör vara rättvisa gentemot de registrerade och öppet redogöra för hur de bedömer och redovisar ett effektivt genomförande av inbyggt dataskydd och dataskydd som standard, på samma sätt som personuppgiftsansvariga redovisar överensstämmelse med dataskyddsförordningen enligt principen om ansvarsskyldighet.
- Den senaste integritetsfrämjande tekniken kan användas som ett mått på i vilken utsträckning kraven på inbyggt dataskydd och dataskydd som standard är uppfyllda, om detta är lämpligt i en riskbaserad strategi. Den senaste integritetsfrämjande tekniken i sig omfattar inte nödvändigtvis skyldigheterna i artikel 25. Personuppgiftsansvariga ska bedöma om åtgärden är lämplig och effektiv för att genomföra principerna om uppgiftsskydd och de registrerades rättigheter.
- Befintliga, äldre system omfattas av samma krav på inbyggt dataskydd och dataskydd som standard som nya system. Om äldre system inte redan uppfyller kraven på inbyggt dataskydd och dataskydd som standard, och ändringar inte kan göras för att uppfylla kraven, uppfyller det befintliga systemet helt enkelt inte kraven i dataskyddsförordningen och kan inte användas för att behandla personuppgifter.
- Artikel 25 sänker inte tröskeln för kraven på små och medelstora företag. Följande punkter kan göra det lättare för små och medelstora företag att iaktta artikel 25:
    - Gör tidiga riskbedömningar.
    - Starta med små behandlingar – och öka sedan successivt omfattningen och svårighetsgraden.

- Sök garantier från producenter och personuppgiftsbiträden om inbyggt dataskydd och dataskydd som standard.
- Använd partner som tidigare har haft goda resultat.
- Samtala med dataskyddsmyndigheter.
- Läs vägledningar från dataskyddsmyndigheter och EDPB.
- Följ i förevarande fall uppförandekoder.
- Sök professionell hjälp och rådgivning.

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)