

Att göra en konsekvensbedömning för dataskydd

Anvisning

Dataskyddsteamet, Helsingfors stad

Helsingfors

Vad är personuppgifter och vad menas med behandling av dem?

Personuppgifter och behandling av dem

- Personuppgifter är all den information som ensam eller tillsammans med andra uppgifter gör det möjligt att identifiera en person
- Med behandling av personuppgifter avses alla åtgärder som riktas till personuppgifter, antingen genom automatisk databehandling eller manuellt.
- Behandling är 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.
- Även om man bara läser uppgifterna utgör det behandling.

Vad är en konsekvensbedömning för dataskydd?

Syftet med konsekvensbedömning för dataskydd

- Syftet med konsekvensbedömning för dataskydd är att identifiera, bedöma och hantera risker i samband med behandling av personuppgifter.
- I EU:s dataskyddsförordning föreskrivs det om konsekvensbedömningen.
- Den personuppgiftsansvarige ska i förväg, redan då behandlingen planeras, bedöma och dokumentera vilka risker som behandlingen av personuppgifter orsakar människorna.
- När riskerna har bedömts ska man förebygga dem med lämpliga skyddsåtgärder.

När ska man göra en konsekvensbedömning?

Identifiering av behovet av konsekvensbedömning

- En konsekvensbedömning är obligatorisk bl.a. då man börjar använda ny teknik, behandlar känsliga eller mycket personliga uppgifter eller behandlar personuppgifter i stor omfattning.
- Konsekvensbedömning ska göras innan en tjänst eller ett system tas i bruk.
- Behovet av att bedöma konsekvenserna identifieras genom att man gör en inledande kartläggning för detta, alltid då man börjar planera en ny process, ett systemköp eller att bygga ett system med stadens egna resurser.
- Om man inte gör en konsekvensbedömning då när man borde ha gjort det, kan den nationella dataombudsmannen anse att det rör sig om dataskadegörelse som avses i strafflagen.

Konsekvens- bedömningens verktyg

Helsingfors stads verktyg för konsekvensbedömning

- Staden har egna verktyg för konsekvensbedömningen. Med dem reder man ut bl.a. vilka personuppgifter som behandlas, på vilken grund de behandlas, var de behandlas, hur uppgifterna skyddas och hur de registrerades rättigheter förverkligas.
- Verktögen är inledande kartläggning, dataskyddets checklista, konsekvensbedömningsverktyget och riskanalysblanketten. Man börjar alltid med den inledande kartläggningen som för en vidare till de andra nödvändiga verktygen.
- Verktöyg och anvisningar finns på Helsingfors stads webbplats.

Inledande kartläggning

Helsingfors

Dataskyddsteamet

När ska man göra en inledande kartläggning

- En inledande kartläggning för konsekvensbedömningen ska alltid göras då man börjar planera en ny process, ett systemköp eller att bygga ett system med egna resurser.
- Den inledande kartläggningen ska göras också då man planerar betydande ändringar i befintliga processer och system.
- I den inledande kartläggningen reder man först ut om personuppgifter behandlas.
- Genom att besvara kartläggningens frågor kommer det fram om man bör bedöma konsekvenserna eller ta hänsyn till dataskyddet med hjälp av checklistan, i det fall att personuppgifter behandlas.

Exempelfrågor i den inledande kartläggningen

- I den inledande kartläggningen svarar man på ja/nej-frågor om personuppgifter behandlas och i så fall hurudana.
- Om man svarar ja på en fråga måste man lämna ytterligare uppgifter.
- Exempelfrågor:
 - Ska staden ta i bruk ny teknologi som inte har använts tidigare?
 - Hanteras känsliga eller i övrigt mycket personliga data?
 - Används personuppgifter för bedömning och analys, såsom profilering och prognostisering?
 - Överförs personuppgifter till tredjeland utanför EU?

Att göra den egentliga konsekvens- bedömningen

Bedömning av konsekvenser

- Om den inledande kartläggningen visar att en konsekvensbedömning ska göras, ska man använda konsekvensbedömningsverktyget.
- Vid bedömningen av konsekvenser har det visat sig att det är bra med verkstäder där man först har ett inledande möte med de inbjudna experter som behövs. På det inledande mötet kommer man överens om ansvarsfördelningen. Efter det inledande mötet ordnas en konsekvensbedömningsverkstad (-städer) där experterna redan på förhand har rätt ut ärenden inom deras ansvarsområden så att man kan dokumentera fakta tillsammans i verktyget.

Inledande möte/deltagare

- Ordförande är den som ansvar för ärendet, "projektchef" (ansvar för tidtabell, ansvarsfördelning m.m.)
- Sakkännare (representant för verksamheten, känner behovet för vilket systemet eller processen skaffas)
- "Användare" (den som använder processen eller systemet, känner till det dagliga jobbet)
- Ansvarig för dataskydd (handleder och ger råd för att göra konsekvensbedömningen och ställa frågor)
- Dataskyddsexpert (berättar vilken säkerhetsnivå som krävs)
- Enligt behov
 - Expert på upphandling (ger råd i upphandlingsprocessen).
 - riskhanteringsexpert

Inledande möte/agenda

- Sammanfattning av projektet, vad man ska göra (ordförande)
- Beskrivning av åtgärderna för behandling av personuppgifter (workshop [dia 19-24], om man vill)
- Konsekvensbedömning:
 - Syftet med konsekvensbedömningen (ansvarsperson för dataskyddet)
 - Presentation av verktyget (ansvarsperson för dataskyddet)
 - Genomgång av kraven (kolumn 2 "krav")
 - Presentation av riskhanteringsverktyget
- Ansvarsfördelning:
 - Anteckna ansvar i verktyget eller mötes-pm (vem fyller i vilken rad i konsekvensbedömningens verktyg).
- Tidtabell
 - Bekräfta tidsåtgång, att göra konsekvensbedömningen tar tid.
 - Avtal om verktygen och tidtabellen för workshops

Konsekvensbedömnings-workshop 1

- Före workshoppen:
 - Varje ansvarsperson fyller i sina egna rader i verktyget, även identifierade risker
 - Vem antecknar riskerna i riskanalysverktyget preliminärt
- I workshoppen
 - Genomgång av konsekvensbedömningsverktyget
 - Var och en presenterar sin egen rad
 - Fattas beslut om vilka risker som tas med i riskanalysens verktyg
 - Gruppen klassificerar riskerna
 - Gruppen fyller i riskanalysen och riskhanteringens åtgärder
 - Tidtabell
 - Avtal om nästa workshop

Konsekvensbedömningens avslutande åtgärder

- Fyll i fliken resumé, utvärdera konsekvensbedömningens slutresultat (alltid).
- Slutrapportering för beslutsfattandet (vid behov)
- Förhandssamråd med dataombudsmannen om riskerna är stora och man inte själv kan minimera dem (vid behov)

Uppgift för konsekvens- bedömningens workshop: beskrivning av behandlingsåtgärder

Beskrivning av behandlings- åtgärderna

- Välj ett system ni känner till där man behandlar personuppgifter.
- Under de översta rubrikerna på plakatet beskriver man vad som hör till dem (varje rubrik har lappar av samma färg)
 - På en post-it-lapp identifieras konkreta delar av behandlingen

1 Vilka personuppgifter behandlas och för vilket ändamål

- Vilka personuppgifter behandlas
 - T.ex. Namn, adress personnummer
- Vad är kategrorier av registrerade
 - T.ex. Kunder, kommuninvånare, arbetstagare
- Vilken är personuppgiftens natur
 - T.ex. Offentlig, sekretessbelagd, känslig
- Vad är personuppgifternas syfte?

Vepa 2

Var lagras och hanteras personuppgifterna?

- Varifrån kommer data och hur rör det sig
- Var lagras det
- Var sker hanteringen (konkret + geografisk vidd)
- Vem behandlar uppgifterna

Vepa 3 Hur och när raderas personuppgifter?

- Har lagringstiden bestämts
 - Utför systemet automatisk radering i slutet av lagringstiden?
 - Ska uppgifterna arkiveras och görs detta elektroniskt?
- Kan man få ut enhetlig data när behandlingen är slut?

Sammanfatta en beskrivning av behandlingsåtgärder

- På bordet finns ett stort plakat
- Rita en helhetsbild av behandlingsåtgärder och placera ut lapparna från vepa 1-3.

Flikar för konsekvens- bedömningens verktyg

Fliken bakgrundsuppgifter

- På fliken bakgrundsuppgifter antecknas grundläggande uppgifter om vilken behandling som planeras.

Kort redogörelse för vilken slags hantering av personuppgifter som planeras:	
Bedömningen gjord av:	
Organisation:	
Bedömningsdatum	

Fliken bedömningstabell

- Fliken bedömningstabell har tre delområden. Dessa är:
 - ❖ En systematisk beskrivning av de planerade åtgärderna
 - ❖ En bedömning av nödvändigheten och riktigheten för personuppgifter
 - ❖ En bedömning av riskerna för den registrerades rättigheter
- Varje delområde har dataskyddskrav som ska bedömas.
- Till följande beskrivs närmare hur man använder kolumnerna i bedömningstabellen.

Kolumnen krav

- I denna kolumn finns de dataskyddskrav som bör beaktas i behandlingen.
- Exempel på krav:

För behandlingen av personuppgifter har det gjorts upp en funktionell beskrivning varav följande framgår:

- Vilka personuppgifter behandlas (namn, personnr, adress osv.)?
- Klassificering av data i systemet (offentlig, hemlig, känslig osv.) - hur raderas data?
- Lagringsperioden för uppgifterna har fastställts enligt deras syfte och de ska raderas när lagringsperioden gått ut (även säkerhetskopiorna). - Vilka uppgifter kan läsas, bearbetas eller raderas?

I avtalet med personuppgiftsbiträdet ingår en dataskyddsbilaga.

När behandling görs för den personuppgiftsansvariges räkning ska den personuppgiftsansvarige anlita endast sådana biträden som har tillräckliga skyddsåtgärder för att verkställa tekniska och organisatoriska åtgärder på så sätt att behandlingen uppfyller kraven i dataskyddsförordningen.

Helsingfors

Dataskyddsteamet

Innan behandlingen av personuppgifter börjar, ska den personuppgiftsansvarige samråda med dataskyddsmyndigheten om konsekvensbedömningen visar att behandlingen skulle orsaka en hög risk för de registrerade, och den personuppgiftsansvarige inte vidtagit åtgärder för att sänka risken.

Till dataombudsmannens byrå ska i så fall lämnas följande för bedömning:

- a) ansvarsområden för de personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden som medverkar vid behandlingen, framför allt vid behandling inom en koncern,*
- b) syfte och metoder för den planerade behandlingen;*
- c) de åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning,*
- d) i tillämpliga fall kontaktuppgifter till dataskyddsombudet,*
- e) konsekvensbedömningen för dataskydd som föreskrivs i artikel 35, och*
- f) all annan information som tillsynsmyndigheten ber om.*

Lagringsperioden för uppgifterna har fastställts enligt deras syfte och de ska raderas när lagringsperioden gått ut (även säkerhetskopiorna).

Datahanterings hela livscykel har planerats redan i början.

Den registrerade har möjlighet att rätta och radera sina egna personuppgifter.

En person har rätt att be att få sina uppgifter raderade. Denna rätt förverkligas när staden inte längre har någon grund att behandla uppgifterna eller om personen återkalla sitt tidigare samtycke för behandlingen.

Beskriv här hur kravet förverkligas

- Här beskrivs hur kravet konkret ska förverkligas och om något lämnas utanför.

- Exempel:

- Krav: Personuppgifter samlas in och behandlas för ett eller flera syften som uttryckligen föreskrivs i lagen, och de behandlas inte senare på ett sätt som är oförenligt med dessa syften.
- Svar: Syftet med personuppgifterna är att ordna och genomföra hälsovård. Personuppgifter hanteras inte i något annat syfte.
- Krav: För behandlingen av personuppgifter har det gjorts upp en funktionell beskrivning varav följande framgår:
 - Vilka personuppgifter behandlas (namn, personnr, adress osv.)?
 - Klassificering av data i systemet (offentlig, hemlig, känslig osv.)
 - Hur raderas data?
 - Lagringsperioden för uppgifterna har fastställts enligt deras syfte och de ska raderas när lagringsperioden upphört (även säkerhetskopiorna).
 - Var kan man se, bearbeta eller radera uppgifter?
- Svar: Behandlingsåtgärden har beskrivits (länk till dokumentet i kolumnen "Länkar"). Dessa ärenden framgår av en beskrivning av behandlingsåtgärder. Vi kommer att precisera uppgifterna om automatisk radering visavi lagringstiden och raderingen.

Länk till detaljerad dokumentation, om på annat ställe

- Om det inte finns en omfattande beskrivning, beskriv här hur kravet förverkligas, i denna kolumn kan du lägga till länkar till viktiga dokument.

Uppfylls kravet? -sarake

- Här görs en bedömning av om den planerade behandlingen är i enlighet med fältet Krav, eller om det har dykt upp risker som kräver riskhantering för att minimeras.
- Om svar ja, är detta delområde okej. Om risker ändå identifieras ska de antecknas i fältet Identifierade risker.
- Om svar nej, gå vidare till fältet Identifierade risker.

Identifierade risker- fältet

- Här listas de identifierade risker som försvårar/hindrar dataskyddet. Riskerna behandlas närmare med hjälp av tabellen Konsekvensbedömning-Risikanalys.
- Råd för att fylla i tabellen riskanalys i detta dokument (dia 35).

Uppfylls kriteriet, kan man gå vidare efter riskhanteringsåtgärder?

- Här bedöms om kravet uppfylls efter att de riskhanteringåtgärder vidtagits som har antecknats i tabellen Konsekvensbedömning-riskanalys.
- Om ja, är detta avsnitt i ordning.
- Om nej, ska man avgöra om man avstår från den planerade behandlingen på grund av för stora risker, eller om det är på sin plats med ett förhandssamaråd som nämns på rad 16. Anvisningar för förhandssamaråd i detta dokument (dia 47).

Obs-kolumnen

- Här antecknas nödvändig extra info och observationer.

Fliken resumé för beslutsfattandet

- På denna flik antecknas
 - Konsekvensbedömningens viktigaste iakttagelser
 - De centralaste stora återstående riskerna och åtgärder för att minimera dem
 - Slutlig bedömning och slutsatser av dem som utfört konsekvensbedömningen.
- På fliken skapas en allmän bild av konsekvensbedömningen också för en sådan läsare som inte har gått igenom konsekvensbedömningens hela dokumentation.

Användning av riskanalysblanketten

Användning av riskanalysblanketten

- Vid konsekvensbedömningen används riskanalysblanketten för att avgöra riskernas konsekvenser och sannolikhet samt dokumentera och följa upp riskhanteringsåtgärderna.
- I kolumnen identifierade risker i konsekvensbedömningens verktyg fyller man i riskernas rubriker. Riskerna behandlas närmare på riskanalysblanketten.
- Till följande beskrivs närmare hur man använder riskanalysblanketten.

Fliken allmänna uppgifter

- På fliken Allmänna uppgifter fyller du i den organisation som gjort upp riskhanteringsplanen samt uppgifter som har ett samband med planen.

Sektor/ Förvaltning/ Affärsverk:			
Enhet:			
Konsekvensbedömningens/riskbedömningens o			
Utförd av:			
Datum			
Senaste konsekvensbedömning utförd:			
Övriga planer och bedömningar kring samma tema	Datum	Deltagare/ utarbetat av	Viktigt

Fliken effektivitet och sannolikhet

- På denna flik presenteras de bedömningskriterier som Helsingfors stad tillämpar för riskernas effekt och sannolikhet.

Effektivitet	
Värde	Följdens allvarlighet
5 Betydande	Riskutfallet gäller särskilda kategorier av personuppgifter, sekretessbelagda personuppgifter, personnummer
	Om risken förverkligas kan en utomstående bearbeta personuppgifterna. Som utomstående kan även a
	Uppgifter behandlas på ett sätt som inte är förenligt med det ursprungliga syftet
	Om risken förverkligas kan det leda till t.ex. identitetsstöld, utpressning, betydar
	Risken medför att kritiska datasystem (t.ex. datasystem med hälsouppgifter) inte kan användas
4 Hög	Riskutfallet kräver omedelbar reaktion
	Den planerade personuppgiftsbehandlingen strider mot lag
	Den registrerade kan inte alls förverkliga sina rättigheter
	Riskutfallet leder till att förtroendet förloras för gott
	En risk för vilken man är skyldig att meddela dataskyddsbudsmannen och de
3 Måttlig	Man planerar en ny verksamhet vars risker är svåra att uppfatta
	Följderna för den registrerade är långvariga (flera månader eller t.o.m. år)
	Risken gäller i liten utsträckning särskilda kategorier av personuppgifter, sekretessbelagda personuppgifter, personnummer
	Om risken förverkligas kan en utomstående bearbeta personuppgifterna. Som utomstående kan även a
	Uppgifter behandlas på ett sätt som inte är förenligt med det ursprungliga syftet
2 Låg	Riskutfallet kan leda till en lindrig ekonomisk skada, att personuppgifterna blir offentliga på ett pinsamt sätt
	Risken medför att okritiska datasystem (t.ex. Datasystem med bibliotekets kunduppgifter) inte kan användas
	Riskutfallet kräver reaktion
	Den planerade personuppgiftsbehandlingen strider mot stadens riktlinjer
	Det är svårt att förverkliga den registrerades rättigheter
1 Liten	Riskutfallet leder till att förtroendet tillfälligt förloras
	En risk för vilken man är skyldig att meddela dataskyddsbudsmannen och den registrerade om en p
	Man planerar en ny verksamhet vars risker är svåra att uppfatta
	Följderna för den registrerade är långvariga (flera månader eller t.o.m. år)
	Risken gäller personuppgifter med låg risk dvs andra data än särskilda kategorier av personuppgifter, sekretessbelagda personuppgifter, personnummer

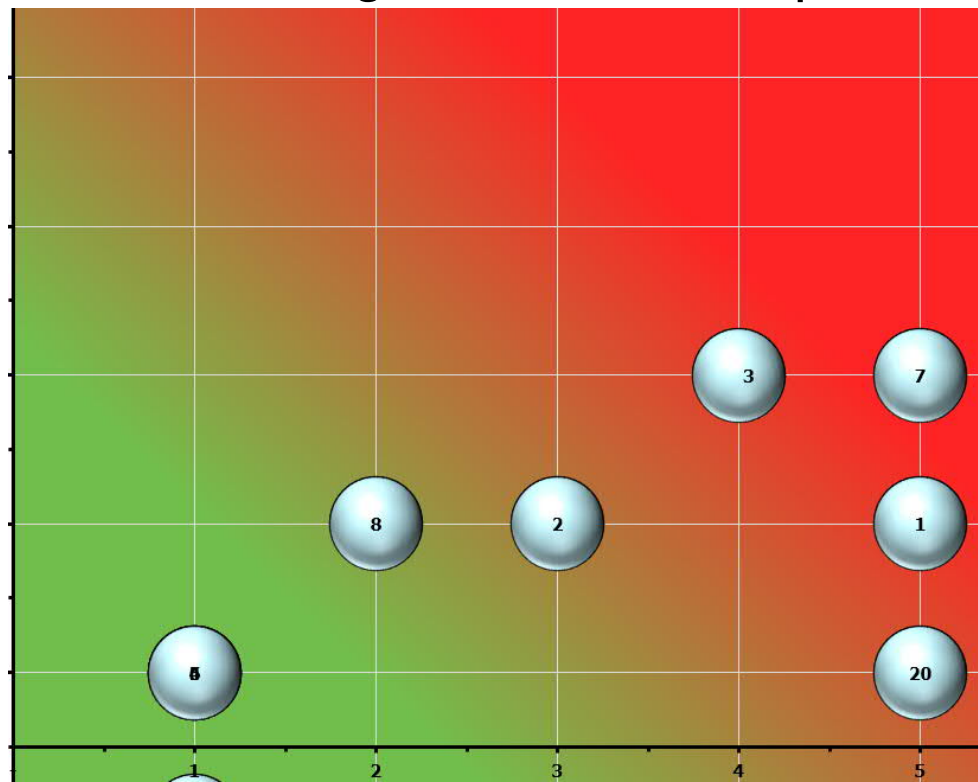
Värde	Klass	Sannolikhet	Frekvens
5	Förväntad	> 90 %	Oftare än en gång per år
4	Ytterst sannolik	< 90 %	En gång på 1-5 år
3	Sannolik	< 60 %	En gång på 5-10 år
2	Osannolik	< 30 %	En gång på 10-20 år
1	Obefintlig	< 10 %	Mer sällan än en gång per 20 år

Fliken riskanalys

- På fliken Riskanalys antecknas identifierade risker per riskklass, dessas sannolika följder om risken förverkligas samt en bedömning av hur allvarliga följderna är och sannolikheten för att de ska förverkligas.
- I en riskanalys är det viktigt att identifiera de faktorer som påverkar riskutfallet eller de händelsekedjor som man försöker påverka genom riskhanteringen.
- För risker som identifierats tidigare fyller man också i kolumnerna "Tidigare risktal" samt "Förändring". Med detta följer man upp att riskhanteringsåtgärderna riktas ändamålsenligt.

Fliken riskbeskrivning

- På denna flik ritas en graf över riskerna enligt allvarlighetsgrad. Riskerna har numrerats med samma nummer i figuren som de är på fliken "Riskanalys".



Fliken Åtgärder för riskhantering

- På den här fliken definieras de åtgärder som minskar eller förebygger sådana risker vars risktal är 8 eller högre eller som på ett annat sätt anses som sådana risker vilka kräver åtgärder. På denna flik filtreras riskerna automatiskt enligt risktalets ordning (det högsta överst).
- Det ska utses en ansvarsperson för riskhanteringen som ser till att åtgärderna vidtas samt den tiddatabell enligt vilken man försöker vidta riskhanteringsåtgärderna. I tiddatabellen bör även antecknas rapporteringspraxis om framsteg i åtgärderna.
- I punkten "Färdighetsgrad" följer man upp hur färdiga de bestämda riskhanteringsåtgärderna är (Inte påbörjad -25% - 50% - 75% - Färdig).

Hur används resultaten från konsekvensbedömningen och riskanalysen?

- Det finns flera olika alternativ för att hantera dataskyddsrisker:
 - Ändringar i en planerad process eller system
 - Organisatoriska styrmetoder
 - Utbildningar, anvisningar, avtal
 - Föregående samråd
 - Vi ber den nationella dataombudsmannen att ta ställning i saken
 - Avstå från projektet
 - Om man inte kan hantera risker med hjälp av de metoder som nämns ovan måste man antingen lägga ner projektet eller planera om det.

Användning av dataskyddets checklista

Användning av checklistan

- Om den inledande kartläggningen visar att personuppgifter kommer att behandlas men att man inte behöver göra en egentlig konsekvensbedömning ska man använda dataskyddets checklista.
- I den finns sådant som alltid ska beaktas under utvecklingen även om man inte behandlar särskilt känsliga eller i övrigt riskabla personuppgifter.

Föregående samråd med dataombudsmannen vid högriskbehandling

När behövs föregående samråd?

- Innan behandlingen av personuppgifter börjar, ska den personuppgiftsansvarige samråda med dataskyddsmyndigheten om konsekvensbedömningen visar att behandlingen skulle orsaka en hög risk för de registrerade, och den personuppgiftsansvarige inte vidtagit åtgärder för att sänka risken.
- När man alltså inte med sina egna riskhanteringsåtgärder kan påverka riskerna som framgår av konsekvensbedömningen, men ändå vill inleda behandlingen är det obligatoriskt med ett förhandssamråd hos dataombudsmannen.
- Behandlingen får inte inledas innan dataombudsmannen gett utlåtande från förhandssamrådet.

Hur görs ett föregående samråd?

- Till dataombudsmannens byrå ska lämnas följande inför förhandssamrådet:
 - a) ansvarsområden för de personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden som medverkar vid behandlingen, framför allt vid behandling inom en koncern,
 - b) ändamålen och medlen för den planerade behandlingen;
 - c) de åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning,
 - d) i tillämpliga fall kontaktuppgifter till dataskyddsombudet,
 - e) konsekvensbedömningen för dataskydd som föreskrivs i artikel 35, och
 - f) all annan information som tillsynsmyndigheten ber om.
- Dataombudsmannen har gett följande instruktioner för förhandssamrådet: <https://tietosuoja.fi/sv/forhandssamrad>



“The processing of personal data should be designed to serve mankind.”

(Recital 4 GDPR)