DATAOMBUDSMANNENS BYRÅ

GÖR UPP ETT DATABOKSLUT

24.4.2012

Guiden uppdaterades i april 2012, och det har inte kontrollerats om den är förenlig med dataskyddsförordningen. Tillämpningen av Europeiska unionens allmänna dataskyddsförordning började 25.5.2018. Information om de rättigheter och skyldigheter som den medför finns på vår webbplats.

www.tietosuoja.fi

INNEHÅLL

1. VAD ÄR ETT DATABOKSLUT

Bokslutet har en lång historia som en form av rapportering av organisationers ekonomiska ställning. Bokslutsrapporteringen har utvidgats till att användas även mer allmänt på organisationers olika delområden både för intern övervakning och organisering av riskhantering. Former av rapportering som kompletterar det ekonomiska bokslutet är företagens och sammanslutningarnas samhälls- och miljöansvarsrapporter samt personalbokslutet. En naturlig uppföljning till denna utveckling är att sträcka granskningen av organisationen genom bokslut till att gälla även datareserver, dataledningskap, databehandling och datasäkerhet.

Databokslutet kan komplettera den lagstadgade rapporteringen som hör till bokslutet och verksamhetsberättelsen men syftet är inte att öka organisationens administrativa börd onödigt. Databokslutets syfte är att fungera som ett dynamiskt verktyg som stöder organisationens effektivitet, påverkan och konkurrenskraft.

Denna guides syfte är inte att presentera en uttömmande mall för eller förteckning över vilka uppgifter som skall omfattas av databokslutet. Databokslutets innehåll kan variera beroende på organisationens verksamhetsområde och verksamhetens kvalitet. Det lönar sig att ta i bruk databokslutet i den omfattning som det upplevs ha positiva effekter på organisationens verksamhet.

Databokslutet är en del av dataledningen och det kan användas som organisationens interna rapport för dataledningen. Med databokslutet kan även rapporteras till organisationens intressentgrupper om centrala ärenden gällande behandlingen av data.

Databokslutet uppstår som ett resultat av den interna granskningen av organisationen och är en rapport som exempelvis:

– ger en helhetsbild över nuläget i organisationens databehandling

– beskriver vilka datareserver organisationen har

– beskriver dataflödet i organisationens verksamhet

– beskriver dataflödets samverkan med databehandlingen

– beskriver hur dataskyddet och datasäkerheten förverkligas i organisationens verksamhet

– beskriver hur riskhanteringen gällande databehandling har förverkligats

– fungerar som stöd vid planeringen och styrningen av verksamheten i organisationen

– fungerar som stöd vid rapporteringen och ledningen i organisationen

– fungerar som hjälpmedel vid uppföljningen av utvecklingsåtgärder

– fungerar som medel för organisationens intressentgruppsrapportering utåt

– försäkrar att den tillämpliga lagen efterlevs

Flera utav de ärenden som skall behandlas i databokslutet omfattas redan av den gällande personuppgiftslagens principer (bl.a. planeringskravet, aktsamhetsplikten och kravet på skydd). Databokslutet förverkligar också den s.k. accountability- d.v.s. redovisningsskyldighetsprincipen. Enligt denna princip skall organisationen själv visa att denne följer lagen, god databehandling och god informationsbehandling. Lagstiftningen gällande dataskyddet kommer i framtiden eventuellt att förutsätta att förfaranden i likhet med principen om databokslutet tas i bruk. Organisationerna kan dock redan på förhand självmant ta i bruk databokslutet. Dokumenteringen i samband med databokslutet styr även till systematisk genomgång av kritisk granskning av ärenden.

2. VARFÖR LÖNAR DET SIG ATT GÖRA ETT DATABOKSLUT

Hög kvalitet av data och fungerande förfaringssätt vid databehandlingen påverkar positivt organisationens alla delområden. Data är en värdefull produktionsfaktor och den enda produktionsfaktorn som är starkt växande. Runt olika datareservrar utvecklas kontinuerligt nya tjänster som är viktiga för hela datasamhällets framgång.

I nät- och datasamhället har databehandlingen en stor betydelse för förverkligandet av personers och organisationers rättigheter och skyldigheter. Exempelvis har Europeiska människorättsdomstolen med sitt beslut NO. 20511/03 bedömt att människorättskonventionen även tillämpas på bedömningen av effekterna av informationssystem. För den offentliga sektorns del har dataskyddet och datasäkerheten blivit bestående delar av god förvaltning. Databehandlingen verkar även väsentligt på konkurrenskraften och organisationers påverkan och effekt.

En förutsättning för nya tjänster och elektroniska serviceprocesser är utvecklandet av datastrukturerna och metoderna i samband med dataadministrationen. Detta skapar nya utmaningar för säker och ansvarsfull databehandling. Som exempel över nya utmaningar kan nämnas köpandet och utnyttjandet av datorkapaciteten och -tjänsterna genom olika s.k. molntjänster. Nuförtiden finns det ett tydligt behov av en heltäckande synpunkt vid förvaltningen av datareservrar, lösningen till detta finns i uppgörandet av databokslut.

Databokslutet beskriver efterlevnaden av god databehandling om vilket stadgas i personuppgiftslagen. För myndigheternas del beskriver databokslutet efterlevnaden av god informationshantering om vilket stadgas i 18 § lagen om offentlighet i myndigheternas verksamhet (621/1999). God informationshantering förutsätter att åtkomsten till, skyddet av och kvaliteten av den behandlade uppgiften tryggas. Med hjälp av databokslutet kan man också bedöma och främja informationssystemens samverkan om vilket stadgas i informationsförvaltningslagen (634/2011).

Erfarenheter har visat att databokslutet är ett särskilt nyttigt medel i myndighetsorganisationen, vars verksamhet grundar sig på behandlingen av stora datareservrar och de registeransvarigas inbördes samarbete.

De mest centrala bestämmelserna från **personuppgiftslagens** synpunkt sett är de allmänna principerna i lagens 2 kapitel:

– aktsamhets- och lagenlighetsprincipen (5 §)

– planeringen av behandlingen av personuppgifter på förhand (6 §)

– personuppgifternas ändamålsbundenhet och begränsningen av behandlingen (7-8 §)

– principer som gäller uppgifternas art (9 §)

Kapitel 7 i personuppgiftslagen innehåller bestämmelser om datasäkerhet, förvaring av uppgifter och skydd av uppgifter.

I databokslutet kan även beskrivas efterlevnaden av annan lagstiftning och exempelvis standardena för datasäkerhet.

2.1. Databokslutet bygger upp förtroendet

Minimering av risker, uppbyggnaden av gott rykte, upprätthållande av medborgarnas och konsumenternas förtroende är faktorer vars betydelse för framgången i alla sektorers verksamhet kommer att öka på ett avgörande sätt. För att främja dessa mål och för att uppnå konkurrensfördel använder sig organisationerna av förfaringssätt som stöder deras verksamhet och gör även mera än vad lagstiftningens minimikrav förutsätter.

Särskilt i nätmiljön upplevs brister i dataskyddet som ett problem med tanke på pålitligheten och användbarheten. Personuppgifter som hamnar i fel händer är ett hot mot objektet för uppgifterna d.v.s. den registrerades rättigheter samt mot verksamheten i organisationen som försummat skyddet av uppgifterna.

Kundernas och intressentgruppernas förtroende till organisationernas förfaringssätt gällande dataskyddet och datasäkerheten stärker verksamheten. Beaktande av dataskyddet och datasäkerheten exempelvis i samband med nättjänster är en i lag stadgad skyldighet men också en väsentlig del av god service.

Databokslutet berättar åt olika intressentgrupper att organisationen upplever det viktigt att satsa på förfaringssätten vid databehandlingen, god databehandling samt god informationshantering.

2.2. Databokslutet är ett verktyg för ledningen

Att göra informationshanteringen till en del av ledningen av organisationen är ett utav de mest betydande utmaningarna för organisationers verksamhet. Ledningen har inte nödvändigtvis en helhetsbild över organisationens informationsarkitektur och de uppgifter som behövs i organisationens verksamhet samt förhållandena dem emellan.

Databokslutet tjänar organisationens ledning i beslutsfattandet samt kundernas och intressentgruppernas behov av information. Databokslutet är även en del av dataledningen och till den tillhörande riskhanteringen och den interna övervakningen.

Regelbunden bedömning av datasäkerheten och dataskyddet är en del av organisationens dataledning. Syftet med bedömningen är att säkra de erbjudna tjänsternas funktionsförmåga och användbarhet, datamaterialets kvalitet och den använda datateknikens säkerhet. Syftet med bedömningen är även att säkra den till produktionen av tjänster anknytande datasäkerhetens lednings- och hanteringssystemsverksamhet.

2.3. Databokslutet är ett hjälpmedel vid intern och extern övervakning

Organisationen bör sörja för att den interna övervakningen sköts ändamålsenligt och tillräckligt. Detta ansvarar organisationens ledning för. Det är till organisationens fördel att effektivt övervaka samt granska databehandlingssystemen genom intern och extern granskning; samtidigt anknyts till detta ett starkt och allmänt lagövervakningsintresse. Genom databokslutet kan man förverkliga båda dessa behov. Databokslutet tjänar även lagövervakningsmyndigheternas behov av information.

Databokslutet uppgörs per uppföljningsperiod vilket möjliggör uppföljningen av de i databokslutet beskrivna och bedömda frågeställningarna. Uppföljningsperioden kan vara ett kalenderår eller någon annan till organisationens behov härstammande tidsperiod. Databokslutet kan sammanknytas från den interna övervakningens och riskhanteringens synpunkt sett till en del av organisationens allmänna förfarande gällande bokslutet och verksamhetsberättelsen, resultatledningen eller resultatrapporteringen.

3. HUR GÖR MAN ETT DATABOKSLUT

Databokslutets syfte är att ge en beskrivning av den nuvarande databehandlingen samt en bedömning av dataskyddets och datasäkerhetens förverkligande. I databokslutet kartläggs även utvecklingsbehov gällande databehandlingen samt de åtgärder som dessa förutsätter.

Databokslutet kan exempelvis beskriva:
– vilka datareservrar organisationen besitter
– hurudan är organisationens dataarkitektur
– hurudan är användbarheten och kvaliteten av de uppgifter organisationen besitter
– vilka förfaringssätt och principer följs vid databehandlingen
– hur skyddas uppgifterna
– hur övervakas databehandlingen
– hur förverkligas de registrerades rättigheter i databehandlingen
Databokslutet innehåller en bedömning av de utvecklingsobjekt och utvecklingsåtgärder som observerats vid databehandlingen.

I uppgörandet av databokslutet kan delta åtminstone de grupper som ansvarar för organisationens datateknik, dataskydd och datasäkerhet samt den egentliga substansverksamheten.

3.1. Uppgifter som skall finnas i databokslutet

De uppgifter som omfattas av databokslutet kan variera beroende på organisationens verksamhetsområde och verksamhetens kvalitet. I det följande ges exempel över faktorer som kan tas med i databokslutet.

3.2. Uppgiftsreservar i organisationens besittning

I organisationen samlas och behandlas uppgifter i flera olika informationssystem och applikationer. Organisationens ledning har inte alltid en uppfattning över vilka uppgifter organisationen besitter. Behandlingen av lösa uppgifter i separata informationssystem kräver rikligt med resurser och bildar ett hot mot förverkligandet av dataskyddet och datasäkerheten.

Från personuppgifternas behandlingssynpunkt sett är det viktigt att bedöma de personregister som bildats för olika användningsändamål, deras datainnehåll och grunderna till upprätthållandet av registren. God informationshantering förutsätter att organisationen har en klar uppfattning över informationssystemen och den bör sörja för uppgifternas kvalitet och tillgänglighet.

Datareservrernas skyddsnivå, sekretess, uppgifternas känslighet är ändamålsenligt att bedöma i samband med kartläggningen av datareservrerna. Kartläggningen av dataflödet mellan datareservrerna är viktigt eftersom förvaltningen av allt större dataflöd lyfter upp frågor om t.ex. datans ägare. Beskrivningen av datareservrerna och dataflödet kan göras för databokslutet eller det kan upprätthållas separat i organisationen som dataarkitekturbeskrivningar eller andra motsvarande beskrivningar.

Databokslutet kan innehålla en beskrivning av organisationens centrala datareservrer och dataflöden samt en bedömning av datans kvalitet. I databokslutet kan även beskrivas de

Databokslutet kan exempelvis beskriva:
– vilka datareservrar organisationen besitter
– hurudan är organisationens dataarkitektur
– hurudan är användbarheten och kvaliteten av de uppgifter organisationen besitter
– vilka förfaringssätt och principer följs vid databehandlingen
– hur skyddas uppgifterna
– hur övervakas databehandlingen
– hur förverkligas de registrerades rättigheter i databehandlingen

Databokslutet innehåller en bedömning av de utvecklingsobjekt och utvecklingsåtgärder som observerats vid databehandlingen.
för databehandlingen viktigaste kontrolltalen, exempelvis antalet behandlade dataenheter, erhållna och utlämnade uppgifter och antalet utlämningar av uppgifter.
Bedömningen av datans kvalitet anknyter sig till bedömningen av datans värde och användbarhet. Datans kvalitet kan i databokslutet bedömas från olika synvinklar, exempelvis:
– förfaringssätt och kriterier vid bedömningen av kvaliteten
– resultaten vid bedömningen av kvaliteten:

- riktighet
- behövlighet
- fullständighet

3.3. Förfaringssätten och principerna vid behandlingen av uppgifter

Förfaringssätten kan beskrivas exempelvis genom:
– på databehandlingen påverkande central lagstiftning
– verksamhetsprinciper
– uppförandekodex
– datasäkerhets- och beständighetsplaner
– övriga anvisningar gällande databehandlingen
– förfaringssätt och avtal gällande utkontraktering av databehandling
– förfaranden och avtal gällande informationssystemens uppehåll och anskaffning

Databehandlingen bör bedömas för hela dess livscykels del. Gällande verksamhetsprinciperna vid databehandlingen kan bedömas exempelvis:
– förfaringssätten gällande erhållandet och utlämnandet av uppgifterna
– förvaltningen av användarrättigheter
– dataskydds- och datasäkerhetskraven särskilt gällande elektronisk dataöverföring.

I databokslutet bedöms ifall organisationens personal har den behövliga informationen om de behandlade uppgifternas offentlighet, sekretess och de förfaranden som skall tillämpas vid skyddet av uppgifterna samt om datasäkerhetsarrangemangen och uppgiftsfördelningen. Det bedöms även hur personalen har fått handledning och utbildning gällande databehandlingen samt hur anvisningarna och utbildningen hålls uppdaterad.

3.4. Skydd av uppgifter

I databokslutet kan beskrivas vilka registeransvariga som genomför de tekniska och organisatoriska åtgärder som behövs för att skydda personuppgifterna mot obehörig åtkomst och mot förstöring, ändring, utlämnande och översändande som sker av misstag eller i strid med lag eller mot annan olaglig behandling.

I databokslutet kan bedömas:
– principerna och förfaringssätten vid skyddet av uppgifterna
– de centrala målen och sätten att uppnå dessa mål gällande datasäkerheten
– de standarder som följs gällande datasäkerhetsförvaltning
– interna och externa evalueringar
– riskhanteringens förfaringssätt
– datasäkerhetens organisation
– ansvar, utvecklingsprocesser och förfaringssätt

3.5. Uppföljning och övervakning av behandlingen av uppgifter

Organisationen bör säkra att bestämmelserna om god databehandling och god informationshantering efterlevs. De åtgärder som god informationshantering förutsätter

förverkligas så att de olika parternas rättsskydd förverkligas.
Övervakningen av databehandlingen kan vara en del av organisationens övriga interna övervakning och riskhantering. Även övervakningens resultat och de åtgärder som vidtagits på basis av dem bör bedömas.

I databokslutet kan bl.a. beskrivas:
– bedömningen och hanteringen av de risker som riktas mot databehandlingen
– de åtgärder som vidtagits för att övervaka datareserverna och dataflödet
– de åtgärder som vidtagits för att övervaka uppgifternas behandlingsprocess
– de åtgärder som vidtagits för att övervaka behandlingen av uppgifterna i organisationens personal och samarbetspartners
– de åtgärder och utvecklingsåtgärder som vidtagits på basis av övervakning och uppföljningen.

Vid sidan av den interna övervakningen kan även beskrivas de beslut som de myndigheter som utför extern laglighetsövervakning och domstolarna fattat under uppföljningsperioden samt deras inverkan på organisationens verksamhet. Dessutom kan i databokslutet bedömas tillräckligheten och utvecklingsbehovet av övervakningen och uppföljningen av databehandlingen.

3.6. Förverkligandet av de registrerades rättigheter

Förverkligandet av de registrerades rättigheter kan bedömas enligt antalet begäran om rätt till insyn eller rättelse av uppgift som gjorts med stöd av personuppgiftslagen samt de svar som givits på dessa framställningar. Gällande informeringen av de registrerade är det skäl att bedöma åtkomsten till register- och dataskyddsbeskrivningarna.

4. BEDÖMNING OCH UTVECKLINGSOBJEKT

I databokslutet identifieras utvecklingsbehov och därtill anknytande uppföljning och rapportering genom att analysera nuläget. Utvecklingsåtgärderna kan gälla exempelvis processen gällande datans kvalitet och databehandlingen. Utvecklingsåtgärderna kan också gälla framgångsrikt ibruktagande av ny teknologi och för övrigt beredskapen att ta ibruk nya medel.

För statsförvaltningens organisations del kan i databokslutet inkluderas uppgifter om hur organisationen har sörjt för de krav som ställs på datasäkerheten i statsrådets förordning (681/2010).

På basis av databokslutet kan dras slutsatser om exempelvis: – verksamheten och databehandlingen varit förenlig med god databehandling och god informationshantering – uppföljningen och övervakningen av databehandlingen har lyckats i enlighet med lagstiftning, bestämmelser och interna anvisningar – i uppföljningen och övervakningen av databehandlingen har uppmärksammats utvecklingsobjekt och avvikelser på grund av vilka separat nämnda åtgärder vidtagits.

I databokslutet konstateras exempelvis:
– de delområden i databehandlingen där det finns utvecklingsobjekt
– utvecklingsobjekten definieras och tillgängliga lösningar bedöms
– under den tidigare uppföljningsperioden förverkligade utvecklingsobjekts framgång bedöms.

Rapporteringen gällande databokslutet kan riktas till organisationens ledning, arbetstagarna, kunderna och andra intressentgrupper eller till myndigheter som utövar laglighetsövervakning. Databokslutet kan även vara till sin karaktär en dynamisk handling vars innehåll kan formas enligt dess målgrupp. Exempelvis kan om skyddet och övervakningen av uppgifterna rapporteras detaljerat till ledningen medan till andra intressentgrupper rapporteras om samma faktorer som en helhetsbedömning.

Personuppgiftslagen och övriga i denna broschyr nämnda lagar hittas i deras helhet i statens lagstiftningsbank på adressen www.finlex.fi. Allmän information om dataskyddet och personuppgiftslagen hittas på dataombudsmannens byrås hemsida (www.tietosuoja.fi). Även anvisningar från ledningsgruppen för statsförvaltningens datasäkerhet (VAHTI), som utsetts av finansministeriet (www.vm.fi) kan utnyttjas då databokslutet förbereds.

För statens organisationers del kan utnyttjas även statsrådets controller för att ge anvisningar gällande bedömningen av den interna övervakningen och riskhanteringen samt bedömningsramen. Databokslutet kan sammanknytas till bedömningen enligt dessa anvisningar, som ett medel för intern övervakning (Statsrådets controller: Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta, VM 23.12.2005, www.wm.fi). Statsrådets controllers rekommendation är användbar också på den privata sektorn som en finsk källa för bedömningen av god riskhantering, vilken grundar sig på den internationellt och allmänt godkända COSO-ERM -modellen och av den till den offentliga sektorn utarbetade INTOSAI GOV -rekommendationen.