VAHTI / Sekretariatet

3.5.2021

Självutvärdering av dataskyddsförordningen

Stödmaterial för god praxis inom digital säkerhet

3.5.2021

Hantering av dokument

Ägare	Myndigheten för digitalisering och befolkningsdata - Ledningsgruppen för den digitala säkerheten inom den offentliga förvaltningen (VAHTI)
Upprättat av	VAHTI-arbetsgruppen 4 Utveckling av dataskydd
Granskat av	VAHTI-sekretariatet
Godkänt av	VAHTI-sekretariatet

Versionshantering

version nr	åtgärder	datum/per-son
0.80	Utkast	25.1.2021 TS
0.90	Utkast	19.4.2021 KR
1.0	Publicerad version	3.5.2021 KR

VAHTI / Sekretariatet

3.5.2021

Innehållsförteckning

Allmänt

Detta dokument är avsett att användas fritt och tillämpas som stödmaterial för att främja självutvärderingen av dataskyddet. Varje organisation ska kontrollera och anpassa detta till sin egen verksamhet, materialet ska inte tas i bruk som sådant.

Vi hoppas att du ger respons på detta stödmaterial:

https://response.questback.com/dvv/digiturvahyvatkaytannotpalaute

Andra kontakter om stödmaterialet:
digiturva@dvv.fi

1 Självutvärdering

1	**Känner du till vilka personuppgifter din organisation behandlar?**	**(uppskattning)**
Närmare beskrivning	• Namn, adress, e-postadress, telefonnummer osv. • Personbeteckning (29 § i arbetsavtalslagen) • Särskilda kategorier av personuppgifter (artikel 9 i dataskyddsförordningen, 6 § i arbetsavtalslagen) • Personuppgifter om straffdomar och förseelser (artikel 10 i dataskyddsförordningen, 7 § i arbetsavtalslagen) • Personuppgifter som omfattas av spärrmarkering • Personuppgifter för personalen (integritetsskyddslagen), kunder, besökare, intressentgrupper	
Hur påvisas	(Berätta med vilka dokument eller annan dokumentation du visar att kravet uppfylls. Om möjligt, lägg till en hänvisning till dokumentationen.)	
Grunderna för kravet	• artikel 4 (1) i dataskyddsförordningen	
Plan	(Nödvändiga åtgärder med tillhörande ansvar, uppgifter och tidtabeller eller var de finns)	
2	**Har de rättsliga grunderna för behandlingen av personuppgifter identifierats?**	

Närmare beskrivning	• Grunder enligt dataskyddsfärordningen
	  ○ Samtycke
	  ○ Avtal
	  ○ Lagstadgad skyldighet (förutsätter att bestämmelsen specificeras)
	  ○ Livsviktiga intressen
	  ○ Allmänt intresse och offentlig makt (förutsätter att bestämmelserna specificeras, att det allmänna intresset specificeras och att den offentliga makten grundar sig på författningar)
	  ○ Berättigade intressen
	• Har de särskilda förutsättningarna för behandlingen beaktats bl.a. i följande fall:
	  ○ Grunder för behandling av särskilda kategorier av personuppgifter
	  ○ Behandling av straffdomar och förseelser
	  ○ Behandling av personbeteckning
	  ○ Behandling av personuppgifter i samband med arbetsavtal	

Hur påvisas		
Grunderna för kravet	• artikel 6, 9 och 10 i dataskyddsförordningen • Arbetsavtalslagen 6 och 29 § • Integritetsskyddslagen kapitel 2, 3, 5, och 6	

Plan		
3	**Känner man till när din organisation är registeransvarig och när den fungerar som handläggare?**	
Närmare beskrivning	• Finns det en process eller en anvisning för att identifiera rollen?	
Hur påvisas		
Grunderna för kravet	• artikel 4 punkt 7-8 i dataskyddsförordningen	
Plan		
4	**Har avtal om behandling av personuppgifter ingåtts och är hanteringen av avtalen i skick?**	
Närmare beskrivning	• Är dataskyddet inbyggt i upphandlingsprocessen? • Har kraven och villkoren för behandlingen av personuppgifter beaktats i avtalen med personuppgiftsbiträdena? • Har en modell för avtalshantering utarbetats? • Har man tagit hänsyn till överföringar till tredje länder?	
Hur påvisas		
Grunderna för kravet	• artikel 28 i dataskyddsförordningen	
Plan		
5	**Känner man igen situationer med gemensamma registeransvariga och har man kommit överens om ansvar för gemensamt registeransvar?**	
Närmare beskrivning	• Identifieras situationer där det är fråga om gemensamt personuppgiftsansvariga? • Har man kommit överens om ansvarsfördelningen mellan de gemensamt personuppgiftsansvariga, från insamling av information till förstöring/arkivering? • Är rollerna och ansvaren tydliga och transparenta för de registrerade?	
Hur påvisas	• Anvisning eller process som hjälper att identifiera gemensamt personuppgiftsansvariga och rollerna i anslutning till dem • Avtal • Kommunikation om roller och ansvarsfördelning till registrerade	
Grunderna för kravet	• artikel 26 i dataskyddsförordningen • Obs! Även anvisning från Europeiska dataskyddsstyrelsen	
Plan		
6	**Har den egna organisationens interna roller och ansvar i anslutning till behandlingen av personuppgifter har identifierats och fastställts?**	
Närmare beskrivning	• Registerägare / ansvarspersoner • Ledningens ansvar • Chefer • Personal	

	• Tillsyn • Dataskyddsombud • Övriga roller (informationshantering, dataskydd, informat-ionssäkerhet, riskhantering, lokalsäkerhet)	
Hur påvisas		
Grunderna för kravet	• ArbL 4.2 § • artikel 37 i dataskyddsförordningen	
Plan		
7	**Har dataskyddsombudets ställning och roll definierats?**	
Närmare beskrivning	• Behovet av att utse ett dataskyddsombud har utretts • Dataskyddsombudets vikariearrangemang i skick, kontakt under frånvaron • Dataskyddsombudets uppgifter och ställning följer lagen	
Hur påvisas	• beslutet om att utse ett dataskyddsombud • T.ex. ställning definieras i förvaltningsstadgan, arbetsord-ningen • Uppgiftsbeskrivning	
Grunderna för kravet	• artikel 37–39 i dataskyddsförordningen	
Plan		
8		
Närmare beskrivning	• Innehåller den information som krävs?	
Hur påvisas		
Grunderna för kravet	• artikel 30 i dataskyddsförordningen	
Plan		
9	**Förverkligas dataskyddsprinciperna i din organisations verk-samhet?**	
Närmare beskrivning	• Laglighet, korrekthet, öppenhet • Ändamålsbegränsning • Uppgiftsminimering • Korrekthet • Lagringsminimering • Integritet och konfidentialitet	
Hur påvisas		
Grunderna för kravet	• (artikel 5 i dataskyddsförordningen)	
Plan		
10	**Vet man i vilka datasystem personuppgifterna behandlas_**	
Närmare beskrivning	• Datasystemportfölj/-register • Dataflödesbeskrivningar • Hjälpfiler/listor	
Hur påvisas		
Grunderna för kravet		
Plan		

11	**Identifieras ostrukturerad information och hur hanteras den?**	
Närmare beskrivning	• Identifiering och hantering av sporadiska, icke-strukturerade elektroniska uppgifter • Informationen behandlas i miljöer där informationens livscykel inte kan kontrolleras med hjälp av metadata. • T.ex. e-postmeddelanden, filer på nätdiskar, Teams-teamens filer, Skype-/Teams-diskussionshistorik	
Hur påvisas		
Grunderna för kravet		
Plan		
12	**Har informationspraxis definierats och följs den?**	
Närmare beskrivning	• Informationens målgrupp samt behandlingens omfattning och karaktär beaktas vid valet av informationspraxis. • Kunna visa att den registrerade har fått information • Är informationen begriplig och tillgänglig?	
Hur påvisas		
Grunderna för kravet	• artikel 12–14 i dataskyddsförordningen • Lagen om digitala tjänster	
Plan		
13	**Finns det en process för att identifiera behovet av en konsekvensbedömning?**	
Närmare beskrivning	• Har det identifierats när konsekvensbedömning eller förhandssamråd ska genomföras? • Finns det en standardiserad process för att identifiera kriterierna?	
Hur påvisas	• Beskrivning av processen	
Grunderna för kravet	• artikel 35 (1) i dataskyddsförordningen	
Plan		
14	**Finns det en process för hantering av personuppgiftsincidenter?**	

Närmare beskrivning	• Finns det en standardiserad process för att hantera och dokumentera kränkningar?
	  ○ Fastställande av kanal för anmälan och ansvarspersoner för behandlingen av anmälningar
	  ○ Myndighetsanmälningar, beslutsansvar för anmälningar
	  ○ Anmälan till registrerade
	• Hur säkerställs personalens förmåga att identifiera säkerhetsincidenter?	

Hur påvisas	• Beskrivning av processen	
Grunderna för kravet	• artikel 33 och 34 i dataskyddsförordningen	
Plan		
15	**Om personuppgifter överförs till tredje land, har förutsättningarna för överföringen utretts?**	

Närmare beskrivning	• Har man förstått vad som avses med överföring till tredjeländer (t.ex. tillgång till information från tredje land)? • Har man identifierat situationer där överföringar till tredje land sker? • Har man i kravdefinitionen beaktat de situationer där överföringar till tredjeländer inte är möjliga? • Har man beaktat överföringar till tredjeländer i hela underleverantörskedjan?	
Hur påvisas	• Villkor för överföring till tredje land	
Grunderna för kravet	• kapitel 5 i dataskyddsförordningen	
Plan		
16	**Finns det nödvändiga interna och externa anvisningar om dataskydd och datasäkerhet?**	

Närmare beskrivning	• Anvisningar om lokalernas datasäkerhet (till exempel personalens och gästernas rörlighet i lokalerna)
	• Anvisningar för behandling av informationsmaterial inklusive till exempel anvisningar om behandling av personuppgifter och sekretessbelagda uppgifter i olika tjänster
	• Finns det nödvändiga anvisningar? Till exempel:
	  ○ Tillgodoseende av de registrerades rättigheter
	  ○ Dataskyddsprinciper
	• Har anvisningarna och processerna förankrats och hur kan det påvisas?	

Hur påvisas	• Godkända, skriftliga anvisningar • Processbeskrivningar	
Grunderna för kravet	• artikel 32 i dataskyddsförordningen • ArbL 4.2 § 2 punkten	
Plan		
17	**Har man sett till att personalens kompetens upprätthålls vad gäller dataskydd och datasäkerhet?**	
Närmare beskrivning	• Har dataskyddet beaktats i personalens utbildning och introduktion? • Har man beaktat särskilda behov i anslutning till olika roller och arbetsuppgifter? • Upprätthåller man kompetensen regelbundet?	
Hur påvisas	• Utbildningsplan • Utbildnings- och introduktionsmaterial	
Grunderna för kravet	• artikel 32 (4) i dataskyddsförordningen • ArbL 4.2 § 3 punkten	
Plan		
18	**Har ovanstående punkter förändrats till verksamhet, kultur och attityder i din organisation?**	
Närmare beskrivning	• Fundera på hur du kan bedöma hur verksamheten, kulturen och attityden förändras i din organisation. • T.ex. enkätundersökningar riktade till ledningen och personalen	

Hur påvisas	• Servicelöfte om beaktande av dataskyddet i organisationens verksamhet • Informationssäkerhetspolicy • Årsklocka • Kompetensmätning	
Grunderna för kravet	• artikel 5 (2) i dataskyddsförordningen	
Plan		