Checklista för Personuppgiftsbehandling

Svaren i checklistan kommer kunna användas för att identifiera gap i personuppgiftsbehandlingen vilket i sin tur ger underlag i förhållande till insatser som krävs för att stänga de identifierade gapen. Checklistan är inte uttömmande och är endast tänkt att användas som ett första hjälpmedel i e-handlarens arbete med att efterleva dataskyddsförordningens bestämmelser. Kartläggningen i denna checklista, juridiska bedömningar (t.ex. i förhållande till den lagliga grunden) och åtgärder som föreslås baserat på svaren i checklistan bör alltid stämmas av med Svensk Handel Juridik för att säkerställa att bedömningarna och åtgärderna är tillräckliga utifrån dataskyddsförordningens bestämmelser.

1. Inventering av personuppgiftsbehandling

Ni bör inventera och dokumentera vilka personuppgifter ni hanterar, hur de samlas in och till vem uppgifterna lämnas ut. Ni kan behöva göra en bred översyn för att ta reda på vilka uppgifter som hanteras inom de olika delarna av er organisation.

- Identifiera i vilken utsträckning ni behandlar personuppgifter i era dagliga arbetsuppgifter
- Identifiera vilka specifika ändamål ni har för en eller flera arbetsuppgifter
- Identifiera vilka personuppgifter som behandlas i förhållande till varje ändamål; denna information ger er underlag för att säkerställa att ni endast använder uppgifter som är nödvändiga för att uppfylla ändamålet
- Identifiera vilka typer av registrerade som berörs av behandlingen; denna information ger er underlag för vilka personer som ska få information om respektive ändamål.

2. Säkerställ den lagliga grunden för personuppgiftsbehandlingen

Den personuppgiftsansvarige är skyldig att säkerställa den lagliga grunden för behandlingen. Ange vilken (eller vilka) laglig grund som ni anser är tillämplig på er behandling i förhållande till varje ändamål som ni har identifierat ovan. Följande lagliga grunder kan bli relevanta:

a) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse

b) Behandlingen är nödvändig för att uppfylla en avtalsförpliktelse i ett avtal som har ingåtts eller kommer att ingås med den registrerade

c) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller

grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, och/eller

d) Den registrerade har lämnat sitt föregående, giltiga, samtycke.

3. Inventering av särskilda kategorier av personuppgifter

Identifiera om ni behandlar s.k. särskilda kategorier av personuppgifter, d.v.s. uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

4. Tillåten behandling av särskilda kategorier av personuppgifter

För all behandling av personuppgifter krävs att någon av de lagliga grunderna (enligt punkt 2 ovan) är tillämplig. Om ni behandlar särskilda kategorier av personuppgifter krävs dessutom att det finns särskild laglig grund för behandling av just den uppgiften (t.ex. i förhållande till uppgifter om facklig tillhörighet eller hälsodata). Utgångspunkten vid behandling av särskilda kategorier av personuppgifter är nämligen att detta är förbjudet. Det finns dock vissa undantag när detta är tillåtet. Följande undantag kan bli relevanta:

a) Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen,

b) Behandlingen är nödvändig för att fullgöra skyldigheter inom arbetsrätten (inklusive inom områdena social trygghet och socialt skydd) i EU eller enligt en medlemsstats nationella rätt,

c) Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk,

d) Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade, och/eller

e) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet.

Ange vilket (eller vilka) undantag som ni anser är tillämpligt på er behandling av särskilda kategorier av personuppgifter i förhållande till varje ändamål som ni har identifierat i punkt 3 ovan.

Motivera även varför ni anser att den valda lagliga grunden är tillämplig på er behandling, t.ex. vilken skyldighet inom arbetsrätten som gör det nödvändigt för er att behandla personuppgifter.

5. Relevans av personuppgifter

Personuppgifter får endast användas om de är nödvändiga för att uppfylla ändamålet. Detta innebär att ni måste bedöma uppgifternas relevans för att uppfylla ändamålet. Baserat på de svar som har angetts i inventeringen av personuppgifter (punkterna 1 och 3):

- Ange hur ni har gjort bedömningen om personuppgifternas är nödvändighet (dvs. relevans) för att uppfylla ändamålet.
- Om ingen bedömning har gjorts; motivera varför uppgifterna är nödvändiga för att uppfylla ändamålet.

6. Korrekthet

Den personuppgiftsansvarige är ansvarig för att säkerställa att personuppgifterna är korrekta och att de hålls uppdaterade.

- Hur säkerställer ni att uppgifterna hålls uppdaterade och hur ofta uppdateras uppgifterna? Infoga gärna exempel på befintliga rutiner.

7. Fritextfält

Som personuppgiftsansvarig är det viktigt att ha kontroll över de personuppgifter som anges i olika IT-system. Detta innebär att ni också måste fundera över de personuppgifter som kan anges i fritextfält.

- Om ni använder er av IT-system som innehåller fritextfält; vilken typ av personuppgifter kan komma att registreras i sådana fritextfält och för vilket ändamål (se punkterna 1 och 3) registreras dessa personuppgifter?
- Har ni några rutiner på plats för att säkerställa vilken typ av information som får anges i fritextfält? Infoga gärna exempel på de rutiner som finns idag.

8. Samtycke

Dataskyddsförordningen ställer högre krav på vad som utgör ett giltigt samtycke. Om ni har gjort bedömningen att viss personuppgiftsbehandling ska baseras på den registrerades samtycke (se punkterna 2 och 4) är det viktigt att säkerställa att de samtycken som har inhämtats/kommer att inhämtas uppfyller förordningens krav.

- Hur har samtycken historiskt inhämtats och sparats?
- Vilken information har lämnats i samband med att samtycke har inhämtats? Infoga gärna exempel på de samtyckesformulär/den information som använts.
- Har ni några rutiner på plats som säkerställer att giltiga samtycken inhämtas i framtiden?

9. Information

Innan ni påbörjar behandlingen av personuppgifter om registrerade är ni skyldiga att ge information om den behandling som kommer att utföras.

- Hur lämnar ni information till registrerade om den behandlingen som utförs?
- Informerar ni registrerade om er behandling i fall där ni har fått uppgifterna från tredje part?

10. Lagring

Personuppgifter får endast sparas under den tid som de är nödvändiga för att uppfylla det relevanta ändamålet. Om uppgifterna blir irrelevanta, t.ex. för att det handlar om gamla uppgifter, ska dessa raderas.

- Ange befintlig lagringsperiod för personuppgifter i förhållande till de identifierade ändamålen (punkterna 1 och 3).
- Om lagringsperioden följer av en rättslig förpliktelse, t.ex. i lag, förordning eller kollektivavtal, ska även detta anges (gärna med hänvisning till relevant lag/förordning/föreskrift).
- Om det inte är möjligt att bestämma en definitiv period för lagring; beskriv de kriterier som ni tillämpar för att bestämma om uppgifterna fortsatt ska sparas eller raderas (inklusive hur ofta sådan gallring görs och vem som tar beslut) och om det finns funktioner att flagga uppgifter för radering.

11. Den registrerades rättigheter

Enligt dataskyddsförordningen har registrerade vissa rättigheter i förhållande till sina personuppgifter. Detta innebär att en registrerad har rätt att:

a) Begära att få tillgång till sina personuppgifter,

b) Begära att felaktiga personuppgifter rättas,

c) Begära att personuppgifter raderas,

d) Begära att behandlingen av personuppgifter begränsas,

e) Begära att personuppgifter som den registrerade har lämnat överförs i ett strukturerat, allmänt använt och maskinläsbart format till en annan personuppgiftsansvarig (s.k. dataportabilitet),

f) Invända mot behandling av personuppgifter (inklusive rätt att invända mot direktmarknadsföring),

g) Återkalla sitt samtycke, och

h) Invända mot automatiserat beslutsfattande (inklusive profilering).

- Infoga gärna de dokumenterade rutiner som ni har på plats idag.

- Hur säkerställer ni att ni hittar all information som relaterar till en registrerad?

12. Mottagare av personuppgifter

Det bör utredas särskilt om ni delar personuppgifterna med tredje part (dvs. med en annan personuppgiftsansvarig såsom ett bolag inom koncernen eller en samarbetspartner) eftersom detta bl.a. kräver att ni informerar de registrerade om denna delning och informerar tredje part om en registrerad utövar sin rätt till rättelse, radering eller begränsning.

- Ange de mottagare av personuppgifter som ni delar personuppgifter med.

13. Personuppgiftsincidenter

Om det sker en personuppgiftsincident har ni som personuppgiftsansvarig en skyldighet att anmäla incidenten till Datainspektionen inom 72 h. Detta gäller förutsatt att incidenten kan innebära en risk för registrerades fri- och rättigheter (dvs. deras rätt till skydd för sina personuppgifter). Ni kan också ha en skyldighet att meddela de berörda registrerade utan onödigt dröjsmål om incidenten kan innebära en hög risk för registrerades fri- och rättigheter (t.ex. risk för bedrägerier eller identitetskapningar).

- Har ni några rutiner på plats för att säkerställa att personuppgiftsincidenter anmäls till Datainspektionen?
- Vem i er organisation är ansvarig för att personuppgiftsincidenter anmäls/meddelas inom de tillämpliga tidsfristerna?

14. Överföring av personuppgifter utanför EU/EES

Utgångspunkten för överföring av personuppgifter till länder utanför EU/EES är att detta är förbjudet om det inte finns en laglig grund för sådan överföring.

- Överför ni personuppgifter till tredje land?[1]
- Om ja, har ni vidtagit några åtgärder för att säkerställa att det finns en laglig grund för sådan överföring?

15. Personuppgiftsbiträden

Ett personuppgiftsbiträde är en tredje part som behandlar uppgifter för er räkning (dvs. uppgifterna får endast behandlas enligt era instruktioner). Om ni använder er av personuppgiftsbiträden finns en skyldighet i lag att ni ska ingå ett personuppgiftsbiträdesavtal.

- Använder ni er av personuppgiftsbiträden?
- Om ja, har ni ingått ett personuppgiftsbiträdesavtal med sådan tredje part?

[1] Notera att detta också gäller för personuppgifter som lagras i en molntjänst om molntjänstleverantörens servrar finns i ett land utanför EU/EES.

- Har ni gjort en bedömning av de säkerhetsåtgärder som personuppgiftsbiträdet har vidtagit för att skydda uppgifterna? Finns det rutiner att löpande kontrollera att personuppgiftsbiträdet följer sina åtaganden?

Senast uppdaterad: 200227

Trygg E-handel
Drottninggatan 56
41107 Göteborg

Svensk Digital Handel
Regeringsgatan 60
111 56 Stockholm

tryggehandel@dhandel.se