PERSONUPPGIFTSPOLICY

Inledning

Denna policy skapades av och för organisationens behandling av personuppgifter.

”Organisationen” är personuppgiftsansvarig.

Uppgift oavsett form, gränssnitt eller miljö som direkt eller indirekt kan hänföras till en fysisk person (som är i livet) räknas enligt personuppgiftslagen som personuppgift.

Syfte och mål

Organisationen ska säkerställa att kunders, samarbetspartners och interna resursers personuppgifter hanteras i enlighet med ändamålet med behandlingen.

Omfattning

Denna policy och tillhörande dokument omfattar de bestämmelser, processer och rutiner som ska gälla för all behandling av personuppgifter inom organisationen – strukturerade som ostrukturerade.

Hantering av personuppgifter ska enbart vara knutna till avtalsförslag och ingångna avtal t.ex. anställningsavtal, leveransavtal etc.

Organisationens behandling av personuppgifter ska uppfylla krav från gällande lagar, förordningar som föreskrifter.

Organisationens behandling av personuppgifter ska uppfylla krav från gällande lagar, förordningar som föreskrifter.

Då dom personuppgifter, vi som företag hanterar, alltid är knutna till affärsförslag, anställningsavtal etc. är det vår tolkning att dessa personuppgifter är knutna till företagets plikt att lagra ingångna avtal och information enligt bokföringslagen. Inga andra personuppgiftsregister eller information förekommer som är bolagets egendom

Policyn antagen 2018-05-14

Skylink AB

Martin Männer VD

Innehållsförteckning

Inledning

Dataskyddsförordningen

Europaparlamentets och rådets förordning (EU) 2016/679 beslutade den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

Rätten till skydd av personuppgifter kommer i grunden genom den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Utifrån dessa har Europeiska Unionens Stadga om de grundläggande rättigheterna 2016/C 202/02 utarbetats, vars 8:e artikel Dataskyddsförordningen bygger på.

Artikel 8 Europeiska Unionens Stadga om de grundläggande rättigheterna

1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.
2. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.
3. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

Dataskyddsförordningen gäller som lag i alla EU:s medlemsländer från och med den 25 maj 2018. Förordningen innehåller 99 artiklar.

Källa: http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen

Förordningstexten i sin helhet:
http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten

Dataskyddsförordningens syfte

Att skydda personuppgifter.

Tillsynsmyndighet

I Sverige är det Datainspektionen som är oberoende tillsynsmyndighet för behandling av personuppgifter. Datainspektionens webbplats: http://www.datainspektionen.se

Checklista

Checklistan på följande sidor är framtagen för att medvetandegöra och förbereda organisationen för omställning då Dataskyddsförordningen (GDPR) ersätter personuppgiftslagen (PUL) den 25 maj 2018.

Checklistan är uppbyggd i följande delar:

Huvudområde

Utgör utdrag av betydande områden för behandling av personuppgifter. Dessa baseras på vägledning från Datainspektionen som i Sverige är tillsynsansvarig myndighet för behandling av personuppgifter. Belyser även skillnader mot gällande personuppgiftslag.

Kravtext

Huvudområdet kopplas till formulering som är baserat på dataskyddsdirektivets krav som det ser ut idag.

Ja (ange på vilket sätt och omfattning, en kryssruta)

Ange svar utifrån frågeställning.

Nej (ange varför och eller vad som behöver göras, en kryssruta)

Ange svar utifrån frågeställning.

Vet ej (ange varför och eller vad som behöver göras, en kryssruta)

Ange svar utifrån frågeställning.

De brister som framkommer genom checklistan i förhållande till skillnader eller avvikelser från Dataskyddsdirektivets krav – bör åtgärdas.

Dataskyddsförordningen

Personuppgiftslagen kommer att ersättas av dataskyddsförordningen och den ställer krav på organisationens behandling av personuppgifter

Vet er organisation om vad dataskyddsförodningen är? ☒ Ja ☐ Nej ☐ Vet ej
Eventuell kommentar till svar Vi har gått igenom vilka register vi har som hanterar personuppgifter (se registerförteckning) utanför tecknade leveransavtal eller anställningsavtal och funnit att vi inte har några aktiva register som avser privatpersoner utöver dom uppgifter vi måste ha enligt dom lagkrav som gäller kring spårbarhet av genomförda transaktioner och levererade avtal.
Har någon analyserat eller kartlagt dagens och kommande förändringars status och påverkan på organisationen, baserat på införandet av dataskyddsförordningen? ☒ Ja ☐ Nej ☐ Vet ej
Eventuell kommentar till svar Då vi inte arbetar utanför B2B segmentet och alltid arbetar med ingångna avtal eller beställningar från våra företagskunder och anställda är det vår tolkning att dom register vi har inte faller under GDPR då dom inte behandlar spårbara personuppgifter
Finns personer utsedda att arbeta som personuppgiftsbiträde eller dataskyddsansvarig inom organisationen? Dataskyddsförordningen ställer krav på befattningar, dess kompetens, resurser och oberoende. ☐ Ja ☒ Nej ☐ Vet ej
Eventuell kommentar till svar Då vi inte hanterar några personuppgifter som kräver GDPRs skydd är det vår tolkning att vi inte har behov av ett personuppgiftsbiträde.

Personuppgifter som behandlas

Personuppgifter behandlas i en organisation i olika syften och gränssnitt

Vet er organisation om vilka personuppgifter som behandlas? Hanteras klassificerade personuppgifter om barn, annat? ☒ Ja ☐ Nej ☐ Vet ej
Eventuell kommentar till svar Dom uppgifter som behandlas är alltid knutna till ett avtal eller avtalsförslag av något slag.
Vet er organisation om var, varför och hur personuppgifterna behandlas? ☒ Ja ☐ Nej ☐ Vet ej
Eventuell kommentar till svar Alla personuppgifter föregås av antingen ett avtal B2B eller ett anställningsavtal. Utöver detta hanteras inga personuppgifter
Har organisationen tillräcklig kunskap om vilka rättsliga grunder som behövs eller krävs för att behandla personuppgifter? Avtal, samtycke, andra bindande ☒ Ja ☐ Nej ☐ Vet ej
Eventuell kommentar till svar Vi hanterar inte personuppgifter i något register
Vilka rutiner finns i organisationen för behandling av personuppgifter? Är rutinerna fastställda? ☒ Ja ☐ Nej ☐ Vet ej
Eventuell kommentar till svar En personuppgiftspolicy, personuppgiftsanmälan samt riktlinjer och register är framtagen. Då inga utöver lagstadgade uppgifter finns samt att eventuella uppgifter aldrig delges annan part är det vår tolkning att inga ytterligare rutiner krävs.

Missbruksregeln

Personuppgiftslagens undantag för att behandla personuppgifter i ostrukturerat material kommer inte att finnas kvar i den nya dataskyddsförordningen

Har organisationen kännedom om hur detta påverkar organisationens sätt att arbeta på i framtiden? Om organisationen fortsatt behandlar personuppgifter enligt denna missbruksregel efter att dataskyddsförordningen träder i kraft den 25:e maj 2018, så kommer detta att betraktas som ett brott mot dataskyddsdirektivet. Organisationen behöver kartlägga, analysera och utreda alternativ behandling av personuppgifter. ☒ Ja ☐ Nej ☐ Vet ej
Eventuell kommentar till svar Vi har inget ostrukturerat material eller register sparat och kommer fortsatt inte ha det.

Vilken information lämnas

Inför behandling av personuppgifter så ställs krav på att lämna information till den som ska registreras, informationen ska avhandla:

- Ändamålet med behandlingen och
- Att den information som delges ska förstås

Har organisationen sett över rutiner för vilken information som ska kommuniceras och eller lämnas till den registrerade inför behandling av dennes personuppgifter? • På vilka rättsliga grunder behandlas personuppgifter • Hur länge personuppgifterna behandlas • Hur den registrerade kan få insyn i vilka personuppgifter som behandlas • Hur rättelse av personuppgifter ändras i händelse av att personuppgifter ändrats eller att felaktiga uppgifter behandlas • Hur den registrerade kan lämna klagomål till personuppgiftsansvarig eller till tillsynsmyndighet • Hur säkerställs det att den registrerade förstår den delgivna informationen • Framtagande av styrning, rutiner ☒ Ja ☐ Nej ☐ Vet ej
Eventuell kommentar till svar Då vi inte har register med personuppgifter som kan granskas ser vi att vi har kontroll över dom uppgifter vi måste ha för vår affärsverksamhet.
Vet organisationen hur den ska informera den som ska registreras? • Hur säkerställer organisationen att den registrerade förstår informationen • Styrning för hantering/behandling av dokumenterad information • Standardtexter för enskilda system/avtal • Ska service eller tjänst som är förknippad med personuppgiftsbehandling utgöra en del av avtal och ansvarsförbindelser ☒ Ja ☐ Nej ☐ Vet ej
Eventuell kommentar till svar Då vi inte för register utöver vad som krävs för våra ingångna avtal och då är kunderna fullt ut medvetna om att ett affärsförhållande har inletts och godkänts.

Registrerades rättigheter

Dataskyddsdirektivet ställer krav på att organisationen ska säkerställa att den registrerades rättigheter

Kan organisationen uppfylla den registrerades rättigheter?
Den registrerades rättigheter är att:

- Få tillgång till sina personuppgifter
- Få felaktiga personuppgifter rättade
- Få sina personuppgifter raderade
- Invända mot att personuppgifterna behandlas/används som är oförenligt med samtycket och ändamålet
- Invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering
- Flytta personuppgifterna - önskad dataportabilitet

☐ Ja ☒ Nej ☐ Vet ej

Eventuell kommentar till svar

Vi har ingen spårbarhet då vi inte har register som handlar om personuppgifter.

Rättsligt stöd

Dataskyddsförordningen ställer krav på att den som behandlar personuppgifter ska ange på vilka rättsliga grunder eller genom vilket stöd behandling av personuppgifter sker

Organisationen behöver kartlägga och utreda vilka rättsliga grunder eller stöd som gäller för sin behandling av personuppgifter. Alla parter ska ha eller kunna ta del av detta, inklusive tillsynsmyndigheten, vilket medför att organisationen måste dokumentera och bevara information. För personuppgiftsbehandling kontrollera följande:

- Har någon i organisationen arbetsuppgifter kopplade till personuppgiftsbehandling, framtagande av bestämmelser eller regler, kartläggning, utredning, myndighetskontakt eller dokumentationsansvar?
  - Ska denna person även utröna rättsliga grunder/stöd för behandling av personuppgifter?
  - Ska relevanta befattningar även vara kravställare för nivå av skydd för personuppgiftsbehandling, informationsansvar och informationsägarskap?

☐ Ja ☒ Nej ☐ Vet ej

Eventuell kommentar till svar

Då vi inte har några personuppgiftsregister ser vi inte behovet av en sådan funktion inom företaget.

Inhämtning av samtycke

Dataskyddsförordningen ställer tydliga krav på att den som behandlar personuppgifter med stöd av samtycke måste kunna visa att:

- Den registrerade förstått och accepterat behandlingen av personuppgifterna
- Ett samtycke har lämnats och eller inhämtats och att samtycket varit otvetydigt

Inhämtar organisationen samtycke för behandling av personuppgifter? Om ja, är denna styrning och rutiner förenlig med dataskyddsförordningen?
Organisationen måste betänka:

- Vilka bestämmelser och rutiner som ska gälla för inhämtning av samtycke
- Bestämma/minimera vilka personuppgifter som är tillräckliga och krävs för behandlingen (räcker det med "en uppgift")
- Hur organisationen kan bevisa hur samtycke har inhämtats eller tagits emot
- Rutiner som berör; prövningar, delgivning av dokumenterad information och dess skydd

☐ Ja ☒ Nej ☐ Vet ej

Eventuell kommentar till svar

Då vi inte hanterar personuppgifter utan ingånget avtal i B2B affärer så är avtalets tecknande av högre rang än samtycke och är således detta samtycke enligt vår tolkning

Personuppgifter om barn

Enligt Dataskyddsdirektivet åtnjuter barn ett upphöjt skydd för behandling av dess personuppgifter. Barns skyddsvärda ställning ska också vägas in vid en intresseavvägning

- Den registrerade förstått och accepterat behandlingen av personuppgifterna
- Ett samtycke har lämnats och eller inhämtats och att samtycket varit otvetydigt

Behandlar organisationen barns personuppgifter?
Behandlas personuppgifter om barn bör organisationen se över rutiner för:

- Särskild styrning och rutiner för inhämtning av samtycke från målsman eller från annan bemyndigad person som bestämmer över andra personer som bär status som icke myndig
- Dokumenterad information och dess skydd

☐ Ja ☒ Nej ☐ Vet ej

Eventuell kommentar till svar

Vi har inga personuppgifter om barn eller enskilda personers hemförhållanden.

Personuppgiftsincidenter

Enligt dataskyddsförordningen finns krav på att organisationen ska ha rutiner för hur personuppgiftsincidenter ska hanteras, dokumenteras och skyddas. Om incidenten kan leda till att personer utsätts för risker såsom diskriminering eller, bedrägerier, eller om personuppgifter används för andra ändamål än vad samtycket medger så ska organisationen även informera de registrerade om händelsen så att de kan vidta nödvändiga åtgärder och eller rapportera till tillsynsmyndigheten inom 72 timmar.

Har organisationen styrning och rutiner för personuppgiftsincidenter?
Organisationen behöver betänka:

- Vilken styrning och rutiner som krävs för att upptäcka, rapportera, utreda, dokumentera och skydda personuppgiftsincidenter
- Vilka rutiner krävs för att informera den registrerade om personuppgiftsincidenten
- Vilken information ska delges den registrerade om vidtagna åtgärder och,
- Vägledande information till den registrerade om hur denne framför klagomål till den personuppgiftsansvarige eller till tillsynsmyndigheten
- Ska den registrerade ha rätt att få kännedom om hur dennes personuppgifter skyddas inom organisationen

☒ Ja ☐ Nej ☐ Vet ej

Eventuell kommentar till svar

Rutin för personuppgiftsincident är framtagen.

Integritetsrisker

Om organisationens personuppgiftsbehandling är förenad med särskilda risker för enskildas fri- och rättigheter ska konsekvensbedömning ske avseende dataskydd enligt dataskyddsförordningen.

Förordningen ställer särskilda krav på den som vill behandla personuppgifter på ett sätt som kan medföra stora integritetsrisker för enskilda. Om organisationens konsekvensbedömning visar att risken för integritetsrisker är hög, så måste organisationen samråda med tillsynsmyndigheten innan personuppgiftsbehandlingen får påbörjas. Det finns också krav på att dataskyddsombud ska finnas vid riskfylld behandling av personuppgifter

Arbetar organisationen idag med riskanalys/säkerhetsanalys för arbetet med behandling av personuppgifter för att identifiera, bedöma och behandla integritetsrisker?
Och hur dessa står i paritet med att uppfylla den registrerades rättigheter och ändamål med personuppgiftsbehandlingen
Organisationen behöver fastställa:

- Hur en konsekvensbedömning för behandling av personuppgifter ska analyseras och hanteras innan behandling av personuppgifter påbörjas
- Hur dokumenterad information ska hanteras och skyddas

☐ Ja ☒ Nej ☐ Vet ej

Eventuell kommentar till svar

Då vi inte har några personuppgiftsregister där detta kan komma att bli aktuellt så ser vi inte heller här behovet av genomföra kontinuerliga risk/säkerhetsanalyser.

Personuppgifter och IT-system

När organisationen behandlar personuppgifter ska lämpliga tekniska och organisatoriska åtgärder vidtas för att uppfylla kraven i dataskyddsförordningen, både när beslut fattas om hur behandlingen ska genomföras och under hela den fortsatta behandlingen av personuppgifterna.

Uppbär organisationens IT-system särskilda funktioner som är avsedda att skydda personuppgifter (för att motverka/förebygga personuppgiftsincidenter)?
Eftersom IT-system som stöd i organisationer vanligen bearbetar personuppgifter, så bör organisationen utarbeta en plan för omställning för varje enskilt system, som gör att organisationen kan behandla personuppgifter och personuppgiftsincidenter på ett ändamålsenligt sätt, betänk:

- I ett enskilt datorsystem kan personuppgifter behandlas med olika ändamål
- I ett enskilt datorsystem kan flera personuppgifter behandlas med olika ändamål
- Hur personuppgifter får hanteras i datorsystem och nätverk
- Vilka personuppgifter krävs
- Avidentifiering, kryptering
- Hur ska arbetet dokumenteras och skyddas

☐ Ja ☒ Nej ☐ Vet ej

Eventuell kommentar till svar

Då vi inte har personuppgifter på annat än våra anställda där ingångna anställningsavtal finns som samtycke för att uppgifterna finns och dessa uppgifter är begränsade avseende access för obehöriga anser vi att vi med råge uppfyller GDPRs krav gällande hantering av våra anställdas uppgifter.

Personuppgiftsansvarig inom organisationen

Förordningen ställer krav på att ett dataskyddsombud ska utses. Det gäller till exempel offentliga myndigheter och organisationer riskfylld personuppgiftsbehandling.

Av Dataskyddsförordningen framgår det att, den person inom organisationen som utses som dataskyddsombud måste ha tillräcklig kunskap om dataskydd och få det stöd och de befogenheter som krävs för att kunna utföra sitt uppdrag på ett effektivt och oberoende sätt.

Har organisationen påbörjat överväga strukturer, organisation och roller för behandling av personuppgifter?

- Se över ett för organisationen möjligt ledningssystem för behandling av personuppgifter
- Krävs ett dataskyddsombud, personuppgiftsombud, personuppgiftbiträde, där de olika rollerna har olika ansvars och arbetsuppgifter i arbetet med behandling av personuppgifter, ska organisationen inrätta en "organisation för behandling av personuppgifter" som inrymmer till exempel dessa roller (vilken annan kompetens kan behövas inom denna organisation: juridisk, säkerhet/skydd m.fl.)

Eftersom omställningen sker med effekt från den 25-maj 2018, så bör organisationen skyndsamt påbörja omställningsarbetet

☐ Ja ☒ Nej ☐ Vet ej

Eventuell kommentar till svar

Då vi inter har några personuppgifter eller register som faller under GDPR beträffande riskfylld personuppgiftshantering i våra system ser vi inte behovet av detta inom vår organisation

Verksamhet i flera länder

Huvudregeln i dataskyddsförordningen är att en organisation endast ska behöva svara inför dataskyddsmyndigheten/tillsynsmyndigheten i ett av EU:s medlemsländer.

Har verksamheten/organisationen verksamhet i flera länder (och utanför EU)?
Organisationen bör betänka:

- Om personuppgiftbehandling sker i flera länder är det viktigt att bedöma vilken dataskyddsmyndighet som ansvarar för tillsynen av de personuppgiftsbehandlingar som sker
- Organisationen bör betänka om var strategiska beslut och strategier om personuppgiftsbehandling ska beslutas inom organisationen och vilken tillsynsmyndighet inom EU som ska utöva tillsyn. Inom EU staterna så har vardera medlemsland en egen tillsynsmyndighet för behandling av personuppgifter. I Sverige är tillsynsmyndigheten Datainspektionen. Då ett företag finns i flera länder och eller världsdelar bör organisationen bestämma vilken tillsynsmyndighet som ska gälla (det vill säga har ett svenskt företag verksamhet i Frankrike och Sverige och behandlar personuppgifter, så bör företaget besluta om det är svensk tillsynsmyndighet som ska utöva tillsyn eller om det ska vara Frankrikes tillsynsmyndighet). Detta är ett strategiskt beslut vilket bör fastställas och dokumenteras och ligga till grund för ett effektivt sätt att behandla personuppgifter inom verksamheten/organisationen

☐ Ja ☒ Nej ☐ Vet ej

Eventuell kommentar till svar