Hantering av personuppgifter enligt GDPR för Stifta AB

Fastställd av styrelsen den 1 januari 2019.

1. Allmänt

Med Företaget avses i detta dokument Stifta AB, org. nr. 559169-5845.

1.1 Bakgrund

Enligt artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02) och artikel 16.1 i Fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt 2012/C 326/01 har varje fysisk person rätt till skydd för dennes personuppgifter. Dessa uppgifter skall behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund.

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (GDPR) har byggts upp som en förbudslag, d.v.s. utan stöd i lag är behandling ej tillåten. Förordningen har utformats till skydd för den personliga integriteten när det gäller hantering och behandling av personuppgifter. Förordningen kompletteras av lag med kompletterande bestämmelser till EU:s dataskyddsförordning och förordning med kompletterande bestämmelser till EU:s dataskyddsförordning samt artikel 29-gruppens vägledning.

Ansvaret för behandlingen av personuppgifter åläggs den som behandlar sådana uppgifter som ansvarar för att behandlingen sker på ett lagligt sätt. I sammanhanget bör förtydligas att GDPR är subsidiär i förhållande till lagar på nationell nivå, vilket innebär att annan lag gäller framför GDPR, t.ex. tryggandelagen, bokföringslagen och annan för verksamheten relevant lagstiftning..

Begreppet ”behandlar” är brett och det omfattar bl.a. insamling, registrering, lagring, bearbetning, spridning, med mera. GDPR är en förordning som är gällande direkt i hela EU vilket underlättar flödet av information EU-länderna emellan.

1.2 Syfte

GDPR har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Denna policy har upprättats inom Företaget för att i möjligaste mån undvika att personuppgifter behandlas felaktigt. Den behandling som företas skall vara förenlig med GDPR. Innan Företaget skall behandla uppgifter måste denna klart och tydligt ha ett bestämt syfte med behandlingen, t.ex. lönehantering, administration m.m.

2. Personuppgifter

All information som kan härledas direkt eller indirekt till en fysisk person som är i livet utgör personuppgifter. Även uppgift om en avliden släkting kan vara en personuppgift om uppgiften anknyter till en levande person, men i normalfallet inte. Endast uppgift om t.ex. en persons födelsedatum utgör inte en personuppgift. Skulle det däremot röra sig om ett personnummer betraktas det i allra högsta grad som en personuppgift. Uppgiften skall således leda till en identifiering/spårbarhet.

GDPR tar huvudsakligt sikte på sådan behandling av personuppgifter som helt eller delvis görs med hjälp av datorer. Även annan behandling av uppgifter som kan vara tillgängliga för sökning eller sammanställning enligt särskilda kriterier (s.k. manuellt register) omfattas av lagen.

GDPR gäller dock inte för behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur, t.ex. upprätta en elektronisk dagbok eller föra ett register över sina vänners adresser och telefonnummer.

2.1 Behandling av personuppgifter

Företaget skall ha som förhållningssätt att endast samla in personuppgifter som är nödvändiga, relevanta och ändamålsmässiga. Behandlingen skall även ske på ett korrekt och riktigt sätt. Uppgifter som anses felaktiga eller ofullständiga med hänsyn tagen till ändamålen med behandlingen skall rättas, blockeras eller raderas. Behandlingen skall ske på ett strukturerat sätt med nödvändig information om personuppgifterna som behandlas.

När en behandling sker av personuppgifter skall det ske i enlighet med GDPR. En behandling är i princip all tänkbar kontakt med en personuppgift (insamling, registrering, lagring, bearbetning, spridning, osv.). Huvudregeln är därför att om Företaget på något sätt haft kontakt med personuppgifter bör det noggrant reflekteras över huruvida den hanteringen varit förenlig med GDPR.

Alla personuppgifter som behandlas (på något sätt hanteras eller finns i Företagets system eller arkiv) skall framförallt genomsyras av de principer som styr GDPR. Dessa principer skall alltid beaktas vid hanteringen av personuppgifter.

- Kundens integritet och konfidentialitet – Personuppgifter skall behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

- Laglighet, korrekthet och öppenhet - Personuppgifterna skall behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. De skall vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

- Ändamålsbegränsning - Personuppgifterna skall samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

- Uppgiftsminimering - Personuppgifterna skall vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

- Lagringsminimering – Personuppgifterna får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Företaget har därför fastställt hur länge personuppgifter måste behandlas enligt lag.

- Ansvarsskyldighet – Företaget är ansvarig för dess hantering av personuppgifter. Anställda i Företaget är insatta i reglerna och uppmärksamma på eventuella kommande förändringar för att verksamheten ska fungera med så bra regelefterlevnad som möjligt.

3. Mål och strategier

Företaget ska betraktas som personuppgiftsansvarig i sin verksamhet när Företaget bestämmer vilka uppgifter som skall behandlas och vad de skall användas till. Den personuppgiftsansvarige är skyldig att föra ett register över de behandlingar som görs och att till Datainspektionen anmäla personuppgiftsincidenter. Företagets dataskyddsombud skall se till att personuppgifterna behandlas korrekt. Det är fortfarande personuppgiftsansvarig som har det slutliga ansvaret för behandlingen.

Företaget är i stor utsträckning att anse som personuppgiftsbiträde för andra stiftelser. Företaget behandlar personuppgifter för den personuppgiftsansvariges räkning. Dessa förhållanden skall juridiskt regleras genom ett skriftligt avtal, ett s.k. personuppgiftsbiträdesavtal.

I de fall Företaget använder sig av ett Personuppgiftsbiträde – som skall behandla personuppgifter för Företagets räkning – skall även ett skriftligt avtal upprättas som reglerar det rättsliga förhållandet dem emellan, men då där Företaget står som personuppgiftsansvarig.

4. Förpliktelser mot den vars personuppgifter behandlas

Företaget har vid begäran från den registrerade en skyldighet att:

• utge information om alla personuppgifter som de har lagrat om den registrerade,

• rätta personuppgifter som är fel och komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen,

• radera personuppgifter som avser den registrerade om uppgifterna inte längre behövs för de ändamål som de samlades in för eller för att uppfylla en rättslig förpliktelse,

• begränsa behandlingen av personuppgifter avseende den registrerade till vissa avgränsade syften,

• underlätta överflyttning av personuppgifter om det är den registrerade själv som har lämnat uppgifterna och behandlingen sker med stöd av ett samtycke eller för att uppfylla ett avtal med den registrerade,

• ge kunden ett beslut av en person i stället för någon form av automatiserat beslutsfattande, inbegripet profilering om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne.

Sådan begäran görs skriftligen till Företaget och skall vara undertecknad av kunden. Begäran skall bemötas inom en månad från det att Företaget tog emot begäran. Företagets ovan listade skyldigheter gäller i den mån dessa skyldigheter inte motsätter annan lag.

5. Bevarandet av personuppgifter

Företaget skall ha som utgångspunkt att endast behålla personuppgifter i den mån det är nödvändigt med hänsyn till de ändamål för vilka de samlades in. Företaget skall endast behålla uppgifterna så länge det behövs för att kunna fullgöra vissa åtagande, t.ex. hantera klagomål.

6. Säkerhet

Företaget skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas utifrån den tekniska lösning som används inom organisationen. Företaget skall alltid ha kundens integritet i fokus och skall vid nya tekniska uppdateringar implementera och säkerställa kundens integritet.

6.1 Incidentrapportering

Med personuppgiftsincident menas en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats av Företaget.

Företaget har en skyldighet genom lag att anmäla personuppgiftsincidenter till Datainspektionen inom 72 timmar från och med att Företaget fick kännedom om personuppgiftsincident i det fall personuppgiftsincidenten sannolikt kan leda till en hög risk för fysiska personers rättigheter och friheter. Denna skyldighet gäller om Företaget är personuppgiftsansvarig. Om Företaget inte lyckas anmäla personuppgiftsincidenten inom 72 timmar skall Företaget motivera orsaken till förseningen. I det fall Företaget är personuppgiftsbiträde och upptäcker incident ska detta skyndsamt meddelas till personuppgiftsansvarig för personuppgifterna som Företaget behandlat för dennes räkning.

Anmälan om personuppgiftsincident skall innehålla följande:

1. personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

2. kontaktuppgifterna till Företagets mest insatta gällande incidenten där mer information kan erhållas,

3. beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och

4. beskriva de åtgärder som Företaget har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Företaget skall dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Om personuppgiftsincidenten sannolikt, med hög risk, skulle äventyra den fysiska personens rättigheter och friheter skall Företaget utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten. Informationen skall vara tydlig och klar och åtminstone innehålla de upplysningar och åtgärder som beskrivs ovan i punkt 2-4. Sådan information behöver dock inte lämnas om:

- dessa personuppgifter är oläsbara för personer som inte har behörighet att få tillgång till personuppgifterna, såsom vid kryptering,

- om Företaget efter incidenten vidtagit åtgärder som säkerställt att den höga risk som tidigare bedömts inte längre sannorlikt kommer uppstå, eller
- om informationslämnandet skulle anses utgöra en oproportionell ansträngning, i sådant fall skall istället allmänheten informeras eller liknande åtgärd vidtas.

7. Strukturerat material – säker hantering

Personuppgifter räknas som strukturerade så fort de görs sökbara, exempelvis genom att du lägger in dem i en databas av något slag. I tidigare lagstiftning behövde inte behandlingen ha ett specifikt ändamål enligt den s.k. missbruksregeln.. Denna har genom GDPR slutat gälla och all personuppgiftshantering skall ske enligt ovan nämnda principer.

Det är viktigt att materialet är strukturerat och finns tydligt angivet var information sparas ned och lagras/arkiveras särskilt om en kund använder sig av rätten att bli glömd. Om en kund begär att personuppgifterna om denne skall raderas är det Företagets skyldighet att radera uppgifterna om det inte är sådan information som av annan lagstiftning eller andra skäl skall sparas. Huruvida det förekommer en dubbelarkivering, trippelarkivering eller liknande av personuppgifter finns det inget uttryckligt hinder emot men Företaget måste veta att personuppgifter om en registrerad finns på dessa två, tre ställen, och ingen annanstans.

Har exempelvis Företaget ingen struktur i sin hantering, som dessutom är svår att söka i, kan en radering av samtliga personuppgifter inte säkerställas. Detsamma gäller även vid fråga om en kund vill flytta sina uppgifter till någon annan (dataportabilitet).

8. Registerföring

Regeln om registerföring grundar sig i att Företaget skall visa att den har kontroll över vilka personuppgifter som behandlas. Sammanfattningsvis skall en bedömning göras om ändamålen skiljer sig, vilken kategori av kunder som registreras för samma ändamål och om dessa uppgifter lämnas vidare. Företaget skall kunna visa att de personuppgifter man behandlar sker i enlighet med de ändamål de samlats in och att de är nödvändiga för uppfyllandet av avtal etc., se separat registermall.

9. Ikraftträdande och fastställande

Dokumentet har upprättats och antagits av styrelsen för Företaget som även tillhandahåller löpande uppdateringar av dokumentet. Senaste antagen version ersätter samtliga tidigare versioner. Dessa riktlinjer skall fastställas och godkännas av Företagets styrelse minst en gång per år även om inga ändringar beslutas. Ansvarig för att dessa riktlinjer uppdateras är styrelsen i Företaget.

10. Uppföljning och efterlevnad

För uppföljning och kontroll av att denna instruktion efterlevs ansvarar styrelsen i Företaget.

******