DATASKYDDFÖRORDNINGEN (GDPR)

- Dataskyddförordningen trädde i kraft 2018-05-25, samtidigt i alla EU-länder
- Dataskyddsförordningen kallas ofta GDPR, en förkortning av General Data Protection Regulation
- Dataskyddsförordningen ersätter i Sverige Personuppgiftslagen (PUL)

Ett av syftena med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. I EU:s stadgar om grundläggande rättigheter uttrycks rätten till respekt för privat- och familjeliv. Här finns en särskild bestämmelse om rätt till skydd för personuppgifter.

Dataskyddsförordningen
har också till syfte att skapa en enhetlig och likvärdig nivå för skyddet
av personuppgifter inom EU så att samma regler gäller i hela unionen.
På svensk nivå finns en grundlagsstadgad rätt till skydd för den personliga integriteten
i samband med behandling av personuppgifter.

1. DATAINSPEKTIONEN

Datainspektionen är ansvarig myndighet i Sverige för Dataskyddsförordningen (GDPR). Fullständig information om GDPR finns på inspektionens hemsida med adress https://www.datainspektionen.se/dataskyddsreformen/.

Datainspektionen kontrollerar att lagar efterlevs, bland annat lagar om behandling av personuppgifter. Kontroller görs framför allt genom så kallad tillsyn. Med tillsyn menas att Datainspektionen genom egna iakttagelser av företag, myndigheter eller organisationer kontrollerar att lagar och förordningar följs. Det sker antingen på plats eller per brev, telefon eller e-post. I de flesta fall är tillsynen planerad men man kan också rycka ut efter klagomål eller tips från enskilda eller uppgifter i massmedia.

Datainspektionen har också en konsultativ roll, man kan ställa frågor och erhålla svar och information inom de områden som inspektionen ansvarar för.

2. PERSONUPPGIFTER, DEFINITIONER

All slags information som kan knytas till en levande fysisk person räknas enligt GDPR som personuppgifter. Typiska personuppgifter är namn och personnummer, men även bilder (foton, video, film), ljudupptagningar, registreringsnummer på en bil och IP-nummer kan vara personuppgifter, kort sagt, så snart en uppgift kan leda till att en nu levande fysisk person kan identifieras, är uppgiften definitionsmässigt en *personuppgift*.

3. REGISTRERING AV PERSONUPPGIFTER

Registrering som kan ske utan samtycke:

1. Uppgifter som behövs för att uppfylla avtal med kunder, till exempel kontaktuppgifter och leveransadress.
2. Uppgifter om juridiska personer och myndigheter faller inte under GDPR, kan därför registreras utan samtycke. Personuppgifter hos juridiska personer som behövs enligt punkt 1. kan också registreras utan samtycke.

Registrering eller åtgärder där samtycke alltid krävs:
1. Registrering av barn under 16 år kräver vårdnadshavares samtycke
2. Alla uppgifter som kan innebära att en levande fysisk person kan identifieras
3. Andra uppgifter, till exempel kunders preferenser för sport, mat, film, musik
4. Lämna över personuppgifter till annan organisation (dataportabilitet)

Uppgifter som aldrig ska registreras

1. Uppgifter om personens religion, politiska åsikter, etniskt ursprung, ras, medlemskap i fackförening, hälsotillstånd, sexuell läggning o. dyl.
2. Registrera aldrig onödiga uppgifter, sådana vi inte behöver.

Ovanstående omfattar ett antal viktiga exempel, för vidare information, se Datainspektionens hemsida.

Dokumentation av personers samtycke till att vi registrerat deras personuppgifter ska finnas arkiverade och tillgängliga så länge som registreringen kvarstår.
Andra personuppgifter som inte särskilt registrerats, till exempel e-post
Personuppgifter förekommer i vissa rutiner, utan att vi noterar eller uppmärksammat dessa som *personregister*. E-post är en sådan rutin. Redan själva epostadressen är oftast en personuppgift. Personuppgifter i anställdas datorer kan också innehålla personregister, till exempel adresslistor. Vi ska därför utveckla riktlinjer och rutiner för hantering av e-post och andra rutiner och system som innehåller personuppgifter utan att vi tidigare uppfattat dessa som personuppgifter.
Personuppgifter som avser anställda. Som arbetsgivare måste man hantera personuppgifter om anställda för att uppfylla lagar och avtal samt andra interna eller externa regelverk. Man måste hantera lönelistor, skattelistor, telefonlistor, inpasseringssystem som kan ha formen av listor med personuppgifter i Dataskyddsförordningens mening. Det kan också förekomma att man registrerar kontaktuppgifter till anhöriga.

4. Arkivering av personuppgifter

Personuppgifter ska inte sparas längre än nödvändigt. När de inte behövs för det syfte de samlades in, ska de tas bort. Datainspektionens tumregel är att personuppgifter ska tas bort senast 12 månader efter det att kundrelationen upphört. Det kan finnas skäl att behålla uppgifter längre, t.ex. garantiåtaganden, bokföringslagen.
Mot den bakgrunden ska Bolaget ha rutiner för att hålla personregistren aktuella. Minst en gång per år ska *Personregisteransvariga* granska, revidera och uppdatera samtliga personregister och anmäla resultatet av genomgången till *Företagsansvarig Dataskyddsförordningen (VD)* som därefter ska lämna en rapport till styrelsen.

5. Fysisk säkerhet och IT-säkerhet

Alla personuppgifter ska skyddas och hanteras så att de inte kommer i obehörigas händer. Kraven på säkerhet gäller såväl manuellt förda register som IT-baserade register. Grundskyddet för maskinella personregister bör minst omfatta följande:

1. Alla datorer ska vara uppdaterade med senaste programvaror
2. Alla datorer ska vara försedda med virusprogram
3. Alla datorer ska skyddas av inloggning med lösenord eller motsvarande
4. Trådlösa nätverk ska vara krypterade och kräva lösenord eller motsvarande vid inloggning
5. Säkerhetskopiering ska ske regelbundet

6. ANSVARSOMRÅDEN SENSOR FONDER AB

För att leva upp till kraven i GDPR ska vi utse tydliga ansvarsområden inom Bolagets verksamhet:

1. *Personuppgiftsansvarig*
   Sensor Fonder AB
2. *Företagsansvarig Dataskyddsförordningen*
   VD
3. *Personregisteransvarig*
   Operativt ansvarig för ett personregister
4. *Personuppgiftsbiträde*
   Uppdragstagare som externt hanterar våra personregister, IT-konsulter, webbhotell, ”molnlagring” o. dyl.
5. *Personuppgiftansvarig*
   Sensor Fonder AB är ansvarigt för alla personregister, oavsett om hanteringen sker internt eller externt hos en konsultbyrå
6. *Företagsansvarig Dataskyddsförordningen*
   Den Företagsansvarige ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt inom egna organisationen men också ge hjälp till medarbetare och kunder som är registrerade i våra personregister, om det behövs. Företagsansvarig har det övergripande ansvaret för Bolagets personregister. Vår bedömning är att vi inte behöver utse och anmäla ett *Dataskyddsombud* med hänsyn till de begränsade personuppgifter och personregister vi har i Bolaget.
7. *Personregisteransvarig*
   Personregisteransvarig har det dagliga, operativa ansvaret för ett eller flera personregister. När samtliga personregister i Bolaget är inventerade, fördelaansvaret för personregister till en eller flera anställda.
8. *Personuppgiftsbiträde*
   Upprätta avtal med konsulter, webbhotell eller andra som hanterar Bolagetspersonregister i externa organisationer.

7. INFORMATION TILL KUNDER, EXTERNA BLANKETTER OCH HEMSIDAN

För att underlätta insamling av *samtycken* till att vi registrerar personuppgifter, ska alla våra blanketter, vid insamling av personuppgifter, förses med en kryss-ruta där samtycke kan lämnas. I anslutning därtill infogas en kort informationstext om innebörden av samtycket samt en hänvisning till en utförlig informationstext på vår hemsida.

På hemsidan infogas en utförlig text om våra rutiner för hantering av personuppgifter och förslagsvis hänvisningar till GDPR på Datainspektionens hemsida. Vi måste i efterhand kunna visa upp dokumentation på att vi erhållit kunders samtycketill registrering av personuppgifter. Därför ska våra arkiveringsrutiner innebära att vi har dokumentation om samtycke arkiverat i minst 12 månader längre än kundförbindelsen varar. Vi ska ha beredskap och rutiner för att tillgodose legala krav på information och åtgärder från kunder som är registrerade i våra personregister. Vi är skyldiga att på begäran lämna ut personuppgifter, rätta felaktiga uppgifter, radera personuppgifter, tillmötesgå invändningar mot hur uppgifter används i direktmarknadsföring, informera om arkiveringstider och på begäran genomföra dataportabilitet.

8. NYHETSBREV OCH MARKNADSFÖRING

Det är legalt att skicka ut nyhets- och marknadsbrev till våra kunder. Dock ska det finnas möjlighet för kunden att avbeställa och säga ”Nej” till flera utskick. Vi måste då respektera kundens vilja.
Vid utskick av nyhets- och marknadsöringsbrev till privatpersoner som inte är kunder, gäller som huvudregel att personuppgifter endast får användas om personen samtyckt till detta på förhand. Det ska alltid finnas möjlighet för personen att avbeställa vidare utskick.

9. PERSONUPPGIFTSBITRÄDEN, AVTAL MED UPPDRAGSTAGARE

Personuppgiftsbiträde är någon som behandlar personuppgifter för *en personuppgiftsansvarigs*
räkning, till exempel ett webbhotell eller en servicebyrå.
Vi måste försäkra oss om att våra personuppgiftsbiträden hanterar våra personuppgifter enligt Dataskyddsförordningen, dels att våra ansvarsområden är klart och tydligt avgränsade genom ett avtal samt att hantering och rutiner är tydligt och klart dokumenterade i avtalet.

10. PERSONUPPGIFTSINCIDENTER, RAPPORTERINGS- & ANMÄLNINGSPLIKT

För att kunna leva upp till skyldigheterna i dataskyddsförordningen är det viktigt att vi har rutiner för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter.
Om vi blir utsatta för dataintrång eller på något annat sätt förlorar kontrollen över de uppgifter vi hanterar, måste händelsen dokumenteras.
Om det är sannolikt att incidenten medför risker för enskildas fri- och rättigheter ska händelsen anmälas till Datainspektionen inom 72 timmar.
Om incidenten kan leda till att personer utsätts för allvarliga risker såsom diskriminering, id-stölder, bedrägerier eller finansiella stölder ska vi även informera de registrerade om händelsen så att de kan vidta nödvändiga åtgärder.