INTEGRITETSPOLICY FÖR SOTARN I MARK

DEN 25 MAJ 2018

Den 25 maj 2018 träder Dataskyddsförordningen i kraft vilket ställer fler krav på hur vi som företag hanterar personuppgifter i vårt arbete. För att möta förändringarna har vi arbetat fram följande dokument med de viktigaste förändringarna och ett nytt sätt att arbeta på.

Innehållsförteckning

Dataskyddsförordningen

En ny EU-lag som ersätter personuppgiftslagen (PuL) för hur behandling av personuppgifter ska hanteras. Förordningen är likadan över hela EU vilket gör att det blir lättare att arbeta med personuppgifter mellan europeiska länder och den ställer dessutom högre säkerhets- och informationskrav än PuL på företag och organisationer som behandlar personuppgifter. Dataskyddsförordningen fokuserar på de registrerades rättigheter till sina uppgifter och lägger därför stor vikt vid dessa rättigheter och de medföljande skyldigheter som de företag som behandlar uppgifter har.

Information

Personuppgifter

En personuppgift är en uppgift som ensamt eller tillsammans med andra uppgifter kan användas av någon för att identifiera en nu levande fysisk person. Företagsuppgifter omfattas alltså inte.

Exempel på personuppgifter är: Personnummer, adress, e-post, telefonnummer, fastighetsbeteckning, medlemsnummer/kundnummer, registreringsnummer, IP-adress och fotografier på personer.

Alla uppgifter som ensamma eller tillsammans med andra uppgifter kan användas för att identifiera en fysisk person är en personuppgift. Det betyder att vi som företag som behandlar uppgifter måste säkra även uppgifter som ensamma inte kan identifiera en person men som i kombination med en eller flera andra uppgifter skulle kunna göra det.

Känsliga personuppgifter

Vissa kategorier av personuppgifter har bedömts vara så känsliga att de bara får behandlas om det finns direkt stöd i lag eller den registrerade har gett sin uttryckliga tillåtelse. Om behandling är tillåten så måste dessutom extra stor hänsyn tas till säkerheten och den registrerades integritet.

Dessa uppgifter är: etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska eller biometriska uppgifter, hälsa eller sexuell läggning.

Det betyder att det är mycket viktigt vid registrering av nya noteringar, ändring av sparade noteringar eller uppgifter att kontrollera att de inte innehåller några känsliga personuppgifter som vi inte har laglig rätt att behandla. Endast om det verkligen är motiverat får en sådan uppgift sparas i datasystemet. Om en kund skriver eller skickar in material som exempelvis innehåller hälsouppgifter och det inte är absolut nödvändigt för utförandet av vårt uppdrag ska inte sådana uppgifter sparas utan raderas efter att eventuella övriga uppgifter noterats i datasystemet.

Behandling

När vi gör något med en personuppgift kallas det för att behandla uppgiften. När en uppgift behandlas måste det ske säkert och med skydd för integriteten för personuppgiften. En behandling är inte bara när vi tar upp information om en fastighet eller ett objekt och läser eller ändrar utan också att lagra uppgiften, när vi först registrerar uppgifterna i systemet eller att ta backup på databasen är att behandla uppgifter.

Vårat ansvar

Ansvaret för att behandlingen av uppgifterna sker korrekt ligger på alla inom företaget med VD och styrelsen som ytterst ansvariga.

Gallring

Vi får inte ha uppgifter i sina datasystem som vi inte har behov av. **”Bra att ha” uppgifter får inte sparas bara för att de är bra att ha.** Det är därför viktigt att inte spara personuppgifter i mejl eller på andra platser än där det skall vara. För fullföljandet av uppdraget mot kommunen kan det krävas att uppgifter sparas. Kommunen uppdrar åt oss att lagra information i kontrollboken.

Rättelse

En person som är registrerad i något av våra datasystem har rätt att få sina uppgifter rättade om de är felaktiga. Det betyder att när en registrerad kontaktar oss och anger att uppgifterna inte är korrekta måste vi utreda om den information som den registrerade menar är felaktig faktiskt är det. Det kan vi exempelvis göra genom att jämföra informationen med folkbokföringen eller andra källor och se om det överensstämmer. Om det visar sig att informationen vi har registrerat är felaktig måste vi rätta den så snart som möjligt.

Vi måste alltid utreda om uppgifterna stämmer men behöver inte ändra om det visar sig att uppgifterna som den registrerade meddelar inte stämmer överens med vad vi vet eller kan se i offentliga register. En kund kan alltså inte tvinga oss att registrera en ny adress om vi anser att den nya adressen inte stämmer.

Radering

En person som är registrerad i något av våra datasystem har rätt att få sina uppgifter raderade om det inte längre finns behov av att ha uppgifterna kvar. Den registrerade måste då kontakta oss och meddela att den vill att vi tar bort all information om personen i våra datasystem.

När en registrerad begär att bli raderad måste vi så snart som möjligt utreda om uppgifterna verkligen ska raderas. Kommer vi fram till att vi inte har behov av uppgifterna längre ska de raderas utan dröjsmål. Om utredningen visar att vi fortfarande har behov av uppgifterna, exempelvis om det krävs för att ha en korrekt kontrollbok, då ska uppgifterna inte raderas.

Registerutdrag

En person som är registrerad i något av våra datasystem har rätt att få ett utdrag ur datasystemet med allt som finns registrerat om personen. Registerutdraget är kostnadsfritt för den registrerade och antingen lämnas ut elektroniskt eller fysiskt, beroende på vad den registrerade önskar. Om personen begär flera registerutdrag i snabb följd har vi rätt att ta ut en ersättning för att lämna ut materialet eller i vissa fall neka att lämna ut uppgifterna. Att neka en sådan begäran kräver dock att vi verkligen kan motivera att det inte är skäligt att lämna ut uppgifterna, så huvudregeln är att vi ska lämna ut det begärda materialet.

Säkerhet som standard

Dataskyddsförordningen kräver att datasystem där personuppgifter behandlas sätter säkerhet främst, inte bara rent tekniskt utan även fysisk säkerhet i lokalerna samt rutiner för hur vi arbetar med personuppgifter i systemet.

Det innebär bland annat att vi har begränsningar i hur användare har rätt att använda systemen. Systemen har därför flera nivåer av säkerhet, anställda kommer endast kunna se de uppgifter de behöver för att kunna genomföra sina arbetsuppgifter.

Missbruksregeln (E-post och löpande text)

Tidigare har löpande text i exempelvis word dokument eller mail i mailprogrammet varit undantaget från personuppgiftsreglerna, så länge behandlingen inte kränkt någon eller missbrukats (därav namnet missbruksregeln).

Detta undantaget försvinner när dataskyddsförordningen införs vilket gör att personuppgifter som finns i sådana program nu måste behandlas med samma säkerhet och integritetstänk som

andra datasystem. Vi får alltså fortfarande ta emot e-post och skriva personuppgifter i excel och word men de måste behandlas på samma säkra och lagliga sätt som all annan personuppgiftsbehandling.

Rätt att behandla uppgifterna

För att få behandla uppgifterna måste vi ha en rättslig grund som tillåter oss att behandla uppgifterna. De rättsliga grunderna är uppräknade i dataskyddsförordningen och inga andra än de som uttryckligen skrivits där är tillåtna.

De grunder som kan bli aktuella för oss är:

- Samtycke från den registrerade
- Behandlingen är nödvändig för att fullgöra ett avtal
- Det finns ett allmänt intresse att tjänsten utförs
- Det finns lagkrav eller myndighetsbeslut som kräver att uppgifterna behandlas
- Vi har ett berättigat intresse att behandla uppgifterna

När det gäller sotning så har vi ett allmänt intresse att behandla uppgiften. Det betyder att det är i samhällets intresse att sotning och brandskydd fungerar som det ska och eftersom att det är en sådan samhällsviktig, och till och med lagstiftad, tjänst är det också tillåtet att behandla personuppgifter i samband med detta.

Kontaktuppgifter för personer som arbetar hos kunder eller leverantörer är också personuppgifter och måste behandlas som sådana. För behandling av sådana uppgifter har vi det som kallas berättigat intresse att behandla uppgifterna. Vid varje ny sådan behandling bedömer vi om vi har större intresse att behålla uppgifterna än vad den registrerade har av att vi tar bort den.

Andra uppgifter i våra system kan ha en annan grund och om en registrerad kontaktar oss med frågor angående rättigheter och skyldigheter enligt dataskyddsförordningen hänvisas personen till den ansvarige för dataskyddsfrågor hos oss

Personuppgiftsbiträden

Vi använder oss av underleverantörer till olika saker i vår verksamhet, exempelvis att trycka och skicka brev. Dessa underleverantörer behandlar ofta personuppgifter som vi samlat in och därmed också ansvarar för. Vi har tecknat personuppgiftbiträdesavtal med samtliga personuppgiftsbiträden.

Personuppgiftsincident

En personuppgiftsincident är när personuppgifter oavsiktligt eller olagligt förstörs, förloras, ändras, sprids eller på annat sätt behandlas på ett sätt som kan skada eller kränka den registrerade.

Exempel på personuppgiftsincidenter är:

- Någon stjäl en dator där personuppgifter är sparade
- Någon tappar bort sin mobiltelefon som är kopplad till jobbmailen och innehåller sparade filer med personuppgifter
- En hacker tar sig in i databasen där alla gäldenärer finns sparade

- En CD skiva med personuppgifter förloras eller förstörs oavsiktligen
- Flera aviseringar med olika mottagare hamnar i ett kuvert som skickas ut till en fastighetsägare
- En anställd raderar felaktigt en person som fastighetsägare
- Telefonväxelsystemet havererar och ingen kan kontakta oss under ordinarie öppettider
- En eller flera datorer får sina hårddiskar krypterade av ett virus

Observera att listan inte är uttömmande och att fler situationer kan kvalificera som personuppgiftsincidenter.

Uppgifter behöver inte vara stulna eller ha kommit obehöriga tillhanda

En uppgift behöver inte vara stulen eller ha skickats till en obehörig för att det ska räknas som en incident. Det räcker exempelvis, som syns i listan, med att uppgifter förstörs trots att de skulle sparas för att det ska kvalificera som en incident.

Om det har hänt någonting med uppgifter registrerade hos oss som det inte var tänkt att det skulle hända kan det vara en personuppgiftsincident. Därför kontrolleras med den ansvarige för dataskyddsfrågor om det uppstår en situation där personuppgifter utsatts för risk.

Vissa incidenter måste rapporteras till myndigheterna
Alla personuppgiftsincidenter måste registreras i våra egna incidentregister men allvarligare incidenter måste också rapporteras vidare. Vid särskilt allvarliga incidenter måste dessutom de registrerade som drabbats informeras.

En allvarlig personuppgiftsincident måste inom 72 timmar från det att vi blir medvetna om incidenten rapporteras till Integritetsskyddsmyndigheten (Datainspektionen). Rapporten är standardiserad en mall för rapportering av personuppgiftsincidenter har tagits fram och finns hos ansvarig för dataskyddsfrågor hos oss

Om personuppgifter skickas fel, försvinner, ändras utan lov eller liknande

Kontaktas **omedelbart** IT-chefen eller ansvarig för dataförordningsfrågor så fort felet upptäcks. Det är mycket viktigt att ansvarig personal får informationen så tidigt som möjligt då tidsfristen att rapportera en incident är kort och börjar löpa direkt när det upptäckts, oavsett vem som upptäcker det.

Vi samlar så mycket information som möjligt om vad som hänt men ändrar eller raderar ingenting innan ansvarig personal kan påbörja utredningen.

Insamlande av samtycke

I vissa situationer bör vi samla in samtycke från den registrerade för att få behandla vissa uppgifter. Exempel på det är om en företrädare för ett företag hör av sig och vill få en faktura skickad till sin privata adress eller när en person vill att vi noterar känsliga uppgifter såsom hälsa och sjukdomstillstånd.

Information visas inte

Gallring av en personuppgift kan ske efter det att informationen är inaktuell, när vår rätt att behandla uppgifterna upphör eller på uppdrag av kommunen. Efter att informationen gallrats finns ingenting kvar, det går därför inte att återskapa informationen i efterhand.

Bilaga 1, Rutin för insamlande av samtycke

2018-05-25, version 1

1. **Verifiera personens identitet.**
2. **Informera om våra kontaktuppgifter:**
   2.1. Sotarn i Mark behandlar dina personuppgifter i enlighet med dataskyddsförordningen. För kontakt med oss kan du antingen ringa 0320-14050, maila på mark@sotare.com eller gå in på vår hemsida www.mark.sotare.com

3. **Informera om villkoren för samtycket.**
   3.1. Dina uppgifter kommer behandlas för att _____ (ange varför vi behandlar uppgifterna, ex. fakturering), vi behandlar dina uppgifter med ditt samtycke.
   3.2. Vi samt våra personuppgiftebiträden, vilka exempelvis hjälper oss med utskrifter av fakturor, kan komma att ta del av dina uppgifter.
   3.3. Uppgifterna kommer att sparas så länge de behövs för att uppfylla ändamålet eller till dess att ditt samtycke återkallas.
   3.4. Du har som registrerad rätt att begära rättelse, radering samt begränsning av behandlingen av dina uppgifter, kontakta oss i sådant fall.
   3.5. Du har närsomhelst rätt att återkalla ditt samtycke, kontakta oss då och meddela detta.

4. **Informera att den registrerade har rätt att klaga till Integritetsskyddsmyndigheten.**
   4.1. Om du inte är nöjd med informationen eller hur vi behandlat dina uppgifter enligt dataskyddsförordningen har du rätt att inge klagomål till Integritetsskyddsmyndigheten.

5. **Notera att den registrerade samtyckt till personuppgiftsbehandling samt informerats om sina rättigheter enligt rutinen.**

Bilaga 2, Rutin vid personuppgiftsincident

IT- Chef och ansvarig för personuppgiftsfrågor

Dick Hålldén

Telefonnummer: 070 - 6778285

_____

När du upptäcker en händelse som kan vara en personuppgiftsincident är det viktigt att du dokumenterar all information du har möjlighet i ärendet.

Ringer exempelvis en gäldenär och berättar att denne har fått en annan persons inkassokrav i brevlådan, din dator blir låst av ett virus eller det av misstag mailats personuppgifter till någon som inte ska ha tillgång till dem är det därför nödvändigt att du antecknar allt du kan om incidenten och därefter kontaktar ansvarig personal. Notera därför namnen och telefonnumret till dem i rutan till höger.

Ansvarig personal utreder sedan incidenten och vidtar därefter de nödvändiga åtgärder som behövs med bedömning av ärendets omständigheter och allvarlighet. Du kan behöva vara behjälplig under utredningen.