Policy för personuppgiftshantering

Syfte

Syftet med denna policy är att säkerställa att Stufvenäs Gästgiferi hanterar personuppgifter i enlighet med EUs dataskyddsförordning (General Data Protection Regulation – GDPR). Policyn omfattar alla behandlingar där personuppgifter hanteras och omfattar såväl strukturerad som ostrukturerad data. Denna policy är förankrad hos alla våra medarbetare.

Tillämpning och revidering

Styrelsen ansvarar för att behandlingen av personuppgifter följer denna policy.
Policyn ska fastställas av styrelsen minst en gång per år och uppdateras vid behov.

Verksamhetsansvariga är ansvarig för att hålla i processen kring årlig uppdatering av policyn till följd av nya och förändrade regelverk.
Denna policy är tillämplig för företagets styrelseledamöter, VD, medarbetare samt uppdragstagare som berörs av vår verksamhet.

Organisation och ansvar

Verksamhetsansvarig har det övergripande ansvaret för innehållet i denna policy samt att den implementeras och efterlevs av verksamheten. Verksamhetsansvarig får delegera ansvaret och implementationen till lämplig person på företaget. Alla medarbetare ansvarar för att de agerar i enlighet med denna policy och vad den vill säkerställa.

Begrepp och förkortningar

Personuppgift – En personuppgift är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Registrerad – Den som en personuppgift avser, det vill säga den fysiska person som direkt eller indirekt kan identifieras genom personuppgifterna i ett register.

Personuppgiftsbehandling – En åtgärd eller kombination av åtgärder beträffande personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering och strukturering.

Personuppgiftsbehandling

Varje personuppgiftsbehandling ska ske enligt följande principer:
•Laglighet.
•Ändamålsbegränsning.
•Uppgiftsminimering.
•Korrekthet.
•Lagringsminimering.
•Integritet och konfidentialitet.

För följande behandlingar (tex mejlhantering internt resp. externt etc) gäller särskilt följande:
•Personuppgifter och annan känslig information ska inte skickas med mejl.
•Våra uppgiftsbehandlingar dokumenteras löpande i Behandlingsregistret.
•Uppföljning och utvärdering av vår hantering av personuppgifter ska ske minst årligen.
•Eventuella incidenter rörande personuppgifter som vi behandlar ska utan dröjsmål rapporteras till verksamhetsansvarig.
•Verksamhetsansvarig ska utan onödigt dröjsmål och senast inom 72 timmar anmäla incidenten till Datainspektionen samt i övrigt vidta nödvändiga åtgärder med anledning av incidenten.
•Våra krav på att personuppgifter hanteras enligt GDPR ska alltid säkerställas vid upphandling och utveckling av IT-lösningar och tjänster, och ska vara en del i kravspecifikationen och eventuella avtal.