Policy Personuppgiftshantering

Företag	Säte	Version
Castanum-Koncernen Samtliga bolag	Sundsvall	1.0
Dokumentansvarig	Gäller fr.o.m	
Per Pettersson-Nåw	2018-05-25	
Reviderad av	Datum	Senast Fastställd av Styrelsen
Koncernledningen	2018-04-18	2018-04-26

1. Inledning och syfte

Syftet med denna policy är att säkerställa att vi hanterar personuppgifter i enlighet med EUs dataskyddsförordning (General Data Protection Regulation – GDPR). Policyn omfattar alla behandlingar där personuppgifter hanteras och omfattar såväl strukturerad data. Lagen träder i kraft den 25 maj 2018.

Denna policy skall vid varje tidpunkt vara förankrad hos berörda medarbetare.

2. Tillämpning och Revidering

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

3. Organisation och Ansvar

VD har det övergripande ansvaret för innehållet i denna policy samt att den implementeras och efterlevs av verksamheten. VD 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.

4. Begrepp

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

5. Personuppgiftsbehandling

- Varje personuppgiftsbehandling ska ske enligt följande principer:
  - Laglighet
  - Korrekthet
  - Uppgiftsminimering
  - Ändamålsbegränsning
  - Lagringsminimering
  - Integritet och konfidentialitet
- Våra uppgiftsbehandlingar dokumenteras löpande i *Behandlingsregistret.*
  I detta skall bl a framgå…
  - De behandlingsaktiviteter vi gör med personuppgifter
  - Syftet med behandlingen
  - Vilka typer av Personuppgifter som behandlas
  - Hur länge personuppgifterna sparas
- Uppföljning och utvärdering av vår hantering av personuppgifter ska ske minst årligen
- Eventuella incidenter rörande personuppgifter som vi behandlar ska utan dröjsmål rapporteras till Administrativ chef. Denne 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.
- För att säkerställa att personuppgiftsbehandling uppfyller GDPR skall vi upprätta ett Biträdesavtal med personuppgiftsbiträden, dvs externa innehavare av våra Personuppgifter.
- Det är viktigt att vi har ett ändamål med lagra personuppgifter. Finns det inget ändamål skall dessa tas bort.
- GDPR ställer tydliga krav på att den som behandlar personuppgifter med stöd av samtycke måste kunna visa att ett samtycke har lämnats.
- Samtliga datorer skall ha skyddade lösenord och alla utnyttjade Servrar vara utrustade med adekvata Brandväggar, för att i möjligaste mån ge skydd för s k Hackerattacker.

6. Den registrerades Rättigheter

De viktigaste Rättigheterna för den registrerade är att…

- få tillgång till sina personuppgifter
- få felaktiga personuppgifter rättade
- få sina personuppgifter raderade
- invända mot att personuppgifterna används för direktmarknadsföring
- invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering
- flytta personuppgifterna (dataportabilitet)

7. Dokument, stöd, och underrutiner

För denna rutin finns följande dokument, stöd och underrutiner:

- *Policy Personuppgiftshantering*
  Ett övergripande dokument (detta) beskriver de riktlinjer vi har kring Personuppgiftshantering. Denna fastställs av årligen av Styrelsen.
- *Rutin Personuppgiftshantering*
  Ett mer detaljerat dokument dels med fakta och dels som beskriver hur vi skall hantera Personuppgifter.
  Detta dokument fastställs löpande i Koncernens Ledningsgrupp.
- *Rutin Personuppgiftsincidenter*
  En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter.
  Separat rutin för detta finns upprättad.
- *Personuppgiftsbiträdesavtal*
  Personuppgiftsbiträde är den som behandlar personuppgifter för den Personuppgiftsansvariges räkning.
  Personuppgiftsbiträdet får bara behandla personuppgifterna enligt givna instruktioner och riktlinjer från den Personuppgiftsansvarige.
  En särskild Avtalsmall finns framtagen för detta ändamål.
- *Behandlingsregister*
  Ett register över Behandlingar av Personuppgifter finns framtaget med instruktioner.

Samtliga dessa dokument och mallar finns sparade på G: 21. GDPR.
Här finns även en mapp per Bolag för bl a Behandlingsregistret.

8. Övrigt

Denna Policy har fastställts i Castanum Förvaltning AB's Styrelse den 26 april 2018.