



Bjärke Stål AB

Policy för personuppgiftshantering

Innehållsförteckning

1	Inledning och syfte.....
2	Tillämpning och revidering
3	Organisation och ansvar
4	Begrepp och förkortningar
5	Personuppgiftsbehandling.....
6	Instruktion gällande anställdas mail i Bjärke Stål AB:s namn.....



1 INLEDNING OCH SYFTE

Syftet med denna policy är att säkerställa att Bjärke Stål AB 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.

2 TILLÄMPNING OCH REVIDERING

Ledningen ansvarar för att behandlingen av personuppgifter följer denna policy.

Policyn ska fastställas av ledningen minst en gång per år och uppdateras vid behov.

VD 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. VD har delegerat implementering av denna policy till ledningen.

Alla medarbetare ansvarar för att de agerar i enlighet med denna policy och vad den vill säkerställa.

4 BEGREPP OCH FÖRKORTNINGAR

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



5 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:
 - Mail sparas som huvudregel i 10 år
 - Tidrapporter inlämnade elektroniskt sparas i 90 dagar.
 - Övriga personuppgifter inskickade via mail sparas som längst i 30 dagar. Uppgifterna sorteras ut och om behövs sparas i aktuellt register.
- 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 VD. VD 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.



6 Instruktion gällande anställdas mail i Bjarke Stål AB:s namn:

Säkerställ att personuppgifterna är korrekta och nödvändiga för ändamålet.

- Innan meddelandet skickas eller dokumentet färdigställs ska den anställde säkerställa att innehållet i ett meddelande eller annat dokument är korrekt, relevant och begränsat till vad som är nödvändigt i förhållande till ändamålet.
- Personuppgifter som inte är nödvändiga för syftet med meddelandet ska inte inkluderas.
- Personuppgifter ska bara delas med kollegor eller andra som är i behov av dem.

Håll isär olika ändamål för behandling av personuppgifter

- För att det ska vara möjligt att göra en ändamålsbaserad uppföljning och gallring av personuppgifter bland ostrukturerat material bör de anställda hålla isär personuppgifter för olika ändamål.
- Innan ett meddelande skickas bör de anställda ta ställning till om det verkligen är relevant att skicka hela e-postmeddelandet till samtliga mottagare, eller om det är enkelt att skicka flera separata meddelanden med innehåll som är bättre anpassade i förhållande till ändamålen med kommunikationen.
- På motsvarande sätt bör anställda överväga när de svarar på eller vidarebefordrar en e-posttråd, dvs där tidigare meddelanden är inkluderade. Skicka hela e-posttråden endast om det är relevant för mottagarna. Den anställde bör även överväga om det är relevant att bifoga eventuella bilagor till samtliga mottagare eller om de kan tas bort.

Den anställdes lagring av personuppgifter

- Om möjligt ska personuppgifter i ostrukturerat material som e-post och mötesanteckningar flyttas till ärendehanteringssystem, tex kundregister etc. Annars bör det ostrukturerade materialet flyttas till särskilda mappar i inkorgen. Syftet är att underlätta gallring och minimering av lagring av personuppgifter hos den anställde. T.ex. kan den anställde spara inkommen e-post i en tillfällig mapp. De anställda bör regelbundet gå igenom innehållet i en sådan "tillfällig"-mapp för att bedöma om meddelandena ska behållas, lagras någon annanstans eller raderas.
- Personuppgifter ska gallras ut när ändamålet med behandlingen slutförts. Därför bör de anställda regelbundet gå igenom sin inkorg och skickat-korg i eposthanteraren för att säkerställa att personuppgifter som ska sparas lagras på rätt ställe och att ostrukturerat material som inte längre behövs raderas.



- Samtidigt kan det finnas giltiga skäl att behålla personuppgifter under långa perioder, t.ex. om informationen är nödvändig i ett befintligt leverantörs- eller kundförhållande eller internt projekt som löper under en längre tid.