



Kategori	Versionsnummer	Ansvarig	Datum
Policy	2026.02.02	Fredrik Melander	2026-02-16

1. Syfte och tillämpning

Denna interna policy beskriver hur Härnösands Plåtslageri AB behandlar personuppgifter om anställda, inhyrda, praktikanter, arbetssökande, kunder och kontaktpersoner i den dagliga verksamheten. Policyn baseras på GDPR (EU 2016/679) och Dataskyddslagen (2018:218) och gäller all behandling i: [imy.se], [riksdagen.se]

- Projektportalen (projekt, personal, tid, lön)
- Fortnox (ekonomi, fakturering, leverantörer, löneunderlag)
- Microsoft 365, inkl. OneDrive och e-post
- Interna arbetsrutiner, listor, register, ritningar och dokumentation

2. Personuppgiftsansvarig

Härnösands Plåtslageri AB, org.nr 559127-2629, är **personuppgiftsansvarig** och ansvarar för att all behandling sker lagligt, öppet och säkert enligt GDPR:s principer.

Kontakt: info@harnosandsplatslageri.se / 0611 - 201 10

3. Grundprinciper (GDPR artikel 5)

Vi följer GDPR:s krav på:

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning – uppgifter används endast för specificerade ändamål
- Uppgiftsminimering – vi samlar bara in det som behövs
- Korrekthet – uppgifter ska vara aktuella
- Lagringsminimering – uppgifter sparas inte längre än nödvändigt
- Integritet och konfidentialitet – säker behandling och skydd mot obehörig åtkomst
- Ansvarsskyldighet – vi dokumenterar och kan visa hur vi följer reglerna

4. Vilka uppgifter vi behandlar

4.1 Personal och inhyrda

- Namn, kontaktuppgifter
- Anställningsavtal
- Behörigheter
- Tidrapporter, frånvaro, löneunderlag
- Kompetenser och certifikat
- Skyddsutrustningsbehov, arbetsmiljöanteckningar
- Personnummer (endast när nödvändigt, se avsnitt 7)

4.2 Projektrelaterade uppgifter

- Projektansvariga

- Montörsuppdrag, tider och arbetsorder
- Kompetenser och ansvarsfördelning
- Fördelning av resurser

4.3 Kunder och leverantörer

- Kontaktpersoner, e-post, telefon
- Offerter, projektbeställningar, fakturor

4.4 Digitala uppgifter

- Systemloggar (Microsoft 365 och Projektportalen)
- IP-adresser, inloggnings, åtkomsthistorik
- Dokument lagrade i OneDrive och Teams

5. Varför vi behandlar uppgifter (ändamål + rättslig grund)

Behandling sker endast när det finns rättslig grund enligt GDPR artikel 6. Vanliga grunder hos oss:

Ändamål	Exempel	Rättslig grund
Personaladministration	anställning, lön, frånvaro, utbildningar	Avtal / rättslig förpliktelse
Projekthantering	resursplanering, tidsrapportering, kundleverans	Avtal / berättigat intresse
Ekonomi & bokföring	fakturering, löneunderlag, kundregister (Fortnox)	Rättslig förpliktelse
Arbetsmiljö	incidentrapporter, riskbedömningar	Rättslig förpliktelse
Rekrytering	hantera ansökningar	Berättigat intresse / samtycke
IT-säkerhet	loggar, åtkomstkontroller	Berättigat intresse

6. Våra system och hur de hanterar data

6.1 Projektportalen (projekt, tid, lön, personal)

Innehåller personaldata, kunddata och projektrelaterad information.

Används för:

- tidsrapportering
- projektdokumentation
- personalplanering
- löneunderlag

All behandling måste följa GDPR:s krav på ändamålsbegränsning och säkerhet.

6.2 Fortnox (ekonomi och lön)

Här behandlas:

- kundregister
- leverantörer
- fakturor
- löneunderlag

Behandling styrs av bokföringslagens krav och GDPR:s principer om laglig grund och lagringsminimering

6.3 Microsoft 365 (OneDrive, e-post, Teams)

- Dokument lagras i OneDrive enligt företagets behörighetsstruktur
- All e-post i Microsoft Exchange
- Åtkomst styrs via Microsofts säkerhetsfunktioner (MFA, roller m.m.)
GDPR kräver att överföringar utanför EU/EES skyddas med adekvat nivå, något som Microsofts EU-dataskyddsravverk uppfyller via standardavtalsklausuler och kompletterande skyddsåtgärder.

7. Behandling av personnummer

Personnummer används endast när klart motiverat, t.ex.:

- Löneadministration (Projektportalen / Fortnox)
- Anställningsavtal
- Arbetsmiljöärenden

Det ska inte förekomma i onödan på listor, utskrifter eller i kommunikation. Detta följer Dataskyddslagen 3 kap. 10 § och IMY:s krav på restriktiv hantering av personnummer

8. Mottagare av personuppgifter

Interna mottagare

- Behörig administrativ personal
- Projektledare
- Ledning

Externa mottagare

- Fortnox (personuppgiftsbiträde)
- Projektportalen (personuppgiftsbiträde)
- Microsoft 365 (biträde)
- Myndigheter (Skatteverket, Försäkringskassan) vid lagkrav

Allt regleras genom biträdesavtal enligt GDPR art. 28

9. Lagringstider

Eftersom lagringstider varierar beroende på typ av information följer vi principen om lagringsminimering (GDPR art. 5.1 e)

Typ av uppgift	Lagringstid
Personal- & anställningsuppgifter	Så länge anställningen består + enligt arbetsrättsliga krav (vanligen 2–10 år beroende på typ av dokument)
Löneunderlag	7 år (bokföringslagen)
Projektdata	Sparas endast så länge projektet kräver det och enligt garanti/ansvarstider
Kundinformation	Så länge kundförhållande pågår + nödvändig tid för bokföring och garanti
Rekryteringsdokument	6–24 månader (längre tid kräver samtycke)
IT-loggar	6–12 månader beroende på behov av IT-säkerhet

Vi genomför regelbundna genomgångar av lagrad data och gallrar/arkiverar enligt dokumenterade rutiner.

10. Säkerhetsåtgärder

- MFA och behörighetsstyrning i Microsoft 365
- Rollstyrda behörigheter i Projektportalen och Fortnox
- Kryptering av lagrade och överförda data
- Regelbundna systemuppdateringar

- Incidenthanteringsrutiner (inkl. rapportering enligt art. 33–34 GDPR)
- Minimerad åtkomst – endast de som behöver uppgifter får tillgång

11. Dina rättigheter som anställd / registrerad

Enligt GDPR har du rätt till:

- Information
- Tillgång ("registerutdrag")
- Rättelse
- Radering (i vissa fall)
- Begränsning av behandling
- Dataportabilitet
- Att invända mot behandling

Begäranden hanteras inom 1 månad.

12. Klagomål

Du har rätt att lämna klagomål till Integritetsskyddsmyndigheten (IMY) om du anser att behandling sker i strid med GDPR.

13. Ändringar av denna policy

Policyn uppdateras vid behov, exempelvis när lag ändras eller nya system tas i bruk.