

# POLICY

## Behandling av personuppgifter

### Ecrucial version

Ecrucial version	Ändrat av	Kommentar
0.1	Leif Gyllsdorff	Första Ecrucial -anpassade versionen baserad på standarddokument från Dokumera
0.2	Leif Gyllsdorff	Vidareutvecklad
0.3	Leif Gyllsdorff	Rättat till header och footer
0.4	Leif Gyllsdorff	Förtydligat några luddiga formuleringar
0.5	Leif Gyllsdorff	Korrigerat felaktighet om Närstående
0.6	Leif Gyllsdorff	Lagt till krav på hantering på hantering hos tillfälliga tjänsteleverantörer
0.7	Magdalena Henriksson	I samband med namnbyte, uppdaterat dokumentet med nytt namn på företaget - från Ecru till Ecrucial.

## Innehåll

Om detta dokument.....	3
Bakgrund .....	3
Syfte .....	3
Vad är GDPR/Dataskyddsförordningen i några korta ord .....	3
Omfattning .....	4
Riktlinjer .....	5
Vilka personuppgifter behandlar vi? .....	5
Hur och när behandlar vi personuppgifter? .....	5
Hur får vi tillgång till personuppgifter? .....	5
Underhåll, rättning, borttag och utdrag av personinformation .....	6
Information till berörd person i samband med hantering av personinformation .....	6
Krav på att personuppgifter behandlas på ett betryggande sätt .....	7
När lämnar vi ut personuppgifter .....	7
Vid misstanke om regelbrott .....	7
Referenser .....	8
Ansvar.....	8

## Om detta dokument

Dokumentet är baserat på ett standarddokument från ett externt företag, Dokumera. Dokumeras versionsnummer finns längst ner på varje sida.

Copyright av det anpassade dokumentet tillhör Ecrucial Consulting Group AB och Ecrucials version anges i versionstabellen ovan.

Dokumentets målgrupp är anställda hos Ecrucial  
Dokumentet får ej distribueras utanför Ecrucial utan att detta är godkänt i förväg av Ecrucial.

Ansvarig för underhåll av dokumentet är Informationssäkerhetsansvarig eller annan av Ecrucials ledning utsedd person.

Dokumentet skall revideras och godkännas av Ecrucials VD minst en gång per år.

## Bakgrund

I samband med att EU fattat beslut om ett nytt tvingande regelverk för att hantera personuppgifter, GDPR på svenska Dataskyddsförordningen, så har Ecrucial tagit fram denna policy.

## Syfte

Syftet med detta dokument är flerfaldigt och innebär att:

- Övergripande sammanfatta de krav som ställs i och med införandet av GDPR/ Dataskyddsförordningen som lag i Sverige 25 maj 2018.
- Övergripande beskriva omfattningen av Ecrucials ansvarsområden vad avser GDPR/ Dataskyddsförordningen
- Utgöra ett övergripande stöd för Ecrucials anställda vid de frågeställningar som kan uppstå. Speciellt med tanke på den aktuella avsaknaden av prejudicerande domar eller liknande.
- Formellt och entydigt dokumentera kravet på att Ecrucial skall efterleva lagar och förordningar

## Vad är GDPR/Dataskyddsförordningen i några korta ord

GDPR/Dataskyddsförordningen, i fortsättningen endast GDPR, är framtaget av EU för att skydda personuppgifter och kvalitetssäkra hanteringen av personuppgifter.

Som ett led i detta har man tagit fram:

- Roller med ansvar och skyldigheter
- Krav vid hantering av personinformation
- Krav på rapportering till myndighet vid informationsläckage
- Införande av sanktionsmöjlighet genom dryga böter, de berömda 4%.

GDPR omfattar alla nu levande personer och innebär kort att vi alla äger informationen om oss själva. Sammanfattningsvis kan det sägas innebära att:

- Vi aldrig ger bort information om oss själva, vi lånar endast ut den.
- Vi har därför rätt att återkalla den, det vill säga bli glömda
- Vi har rätt att kräva att den endast används till det den är utlånad för.  
Produktionsdata i test är därför ett no-no
- Vi har rätt att få reda på vilken information en organisation har om oss
- Vi har rätt att få information om oss korrigerad om den är fel eller inaktuell
- Det finns inga krav på att ange ett skäl till varför vi eventuellt inte vill låna ut information eller varför vi vill bli glömda.  
Det är strikt opt-in som gäller.

Undantaget från ovanstående är det som går under 'legal grund', det vill säga någon form av avtalsförhållande som kräver att part lagrar personinformation om annan part.  
Banker är t.ex. restriktiva med att låna ut pengar till personer de ej kan identifiera.

Observera att ovanstående sammanfattning inte är något annat än just en sammanfattning, för en uttömmande beskrivning av GDPR hänvisas till officiell dokumentation se länk under avsnitt Referenser nedan.

## Omfattning

Dokumentet omfattar den personinformation som Ecrucial-anställda eller av Ecrucial direkt inhyrd personal hanterar i av Ecrucial ägd miljö eller där Ecrucial ansvarar för miljön.

Detta innebär att:

- Personinformation som ej ägs eller ansvaras för av Ecrucial men hanteras av Ecrucial -personal på datorer eller i miljöer som ägs och administreras av kund, sådan information omfattas ej.  
Då gäller kunds regelverk med de ansvarsåtaganden som Ecrucials personal har enligt avtal gentemot kund.  
I detta fall är viktigt att vara medveten om och hantera de ansvarsproblem som kan uppstå i samband med en potentiell hantering och lagring av kunds Person- eller annan information på Ecrucial-dator, egen personlig dator eller publik dator.
- Personinformation som hanteras av Ecrucial-personal på datorer eller i miljöer som ägs och administreras av Ecrucial omfattas.  
I detta fall är det viktigt att vara medveten om komplikationerna i samband med en potentiell hantering och lagring av Ecrucial-relaterad personinformation på kunddator, egen personlig dator eller publik dator.

## Riktlinjer

### Vilka personuppgifter behandlar vi?

Vi behandlar endast personuppgifter när det finns laglig grund (för beskrivning av vad laglig grund är se separat dokument under Stödjande Dokument på Intranätet), hantering krävs enligt avtal eller medgivande om hantering finns.

Vi behandlar inte personuppgifter på annat sätt eller i annat fall än när de behövs för att fullgöra förpliktelser enligt ovanstående, d.v.s. lag, avtal eller medgivande.

Nedan följer exempel på generella personuppgifterna vi behandlar:

- Namn
- Adress
- E-postadress
- Telefonnummer
- Titel
- Användarnamn
- Fotografier
- Uppgifter som du registrerade självmant och frivilligt uppger
- Innehåll som du själv publicerar, s.k. användargenererat innehåll

För anställda tillkommer:

- Födelsedatum
- Kön
- Kontaktinformation till anställds närstående
- Bankrelaterade uppgifter för utbetalning av lön och ersättningar

### Hur och när behandlar vi personuppgifter?

Som tidigare uttalats så behandlar vi endast personuppgifter när vi har laglig grund, hantering krävs enligt avtal eller medgivande om hantering finns.

Personuppgifter får ej hanteras av andra skäl eller i andra sammanhang än vad som omfattas av lag, avtal eller medgivande.

Det vill säga att 'för test' eller 'bra att ha' är inte tillåtet.

Notera också konsekvenserna i samband med videofilmning av seminarier vilket kräver samtycke om inte kameran är strikt riktad mot föredragshållaren.

I de fall tillfälliga tjänsteleverantörer används, t.ex. i samband med resor eller event, så är ett krav från Ecrucial att personidentifierande material skall tas bort ur leverantörens register.

### Hur får vi tillgång till personuppgifter?

I samband med avtal där informationen krävs för att Ecrucial skall kunna fullgöra sina åtaganden.

Exempel på det är:

- Anställningsavtal  
I samband med anställning så har Ecrucial ett önskemål om att ha kontaktuppgifter till närstående.
- Uppdragsavtal

Utöver avtalssituationer kan Ecrucial också få tillgång till personuppgifter på följande sätt:

- Uppgifter som vi får när person anmäler sig till Ecrucials kurser eller seminarier
- Uppgifter som vi får när person anmäler sig till nyhetsbrev och andra utskick
- Uppgifter som vi får när person svarar på enkäter och undersökningar
- Uppgifter som registreras när person besöker vår hemsida
- Uppgifter som vi får från offentliga register eller sociala medier
- Uppgifter som vi får när person kontaktar Ecrucial, söker anställning hos Ecrucial, besöker Ecrucial eller på annat sätt tar kontakt med Ecrucial

Notera att samtycke alltid skall inhämtas om det är möjligt innan personuppgifter lagras och börjar behandlas.

Se nedan under Referenser för länk till medgivandedokument.

Om det visar sig omöjligt att få till ett medgivande skall därför dokumenteras vilka försök som gjorts och varför dessa ej lyckats.

Alternativet är att ta bort information om det saknas avtal eller laglig grund.

## Underhåll, rättning, borttag och utdrag av personinformation

GDPR som lag ger person som lånat ut sina personuppgifter ett antal rättigheter:

- Rätten att få reda på vilka personuppgifter Ecrucial har i form av registerutdrag
  - Rätten att få felaktiga uppgifter rättade
  - Rätten att bli glömd
- Rätten att bli glömd gäller dock inte om det påverkar Ecrucials möjligheter att uppfylla skyldigheter enligt avtal eller lag.

I samtliga av ovanstående fall gäller:

- Personen i fråga behöver inte ange något skäl till begäran
- Det åligger inte Ecrucial att med någon form av regelbundenhet fråga om informationen är korrekt

Notera dock att om informationen finns av något specifikt skäl och skälet upphör att gälla så upphör även skälet till att lagra informationen, informationen skall därför rensas bort.

## Information till berörd person i samband med hantering av personinformation

I samband med att vi samlar in personuppgifter för första gången skall personen i fråga informeras om:

- Hur vi har fått tag i personuppgifterna
- Vad vi kommer att använda dem till
- Vilka rättigheter personen har enligt dataskyddslagstiftningen
- Hur dessa kan tas tillvara.
- Vem som är ansvarig för personuppgiftsbehandlingen

- Hur man kan kontakta Ecrucial för frågor eller om man avser lämna en begäran eller förfrågan avseende personuppgifter och/eller rättigheter.  
Den rekommenderade kontaktmetoden är ett mail till [info@ecru.se](mailto:info@ecru.se)

### **Krav på att personuppgifter behandlas på ett betryggande sätt**

Rutiner och arbetssätt skall anpassas så att personuppgifter ska hanteras på ett säkert sätt. Utgångspunkten är att endast arbetstagare och andra personer inom Ecrucial som behöver personuppgifterna för att utföra sina arbetsuppgifter ska ha tillgång till dem.

### **När lämnar vi ut personuppgifter**

Personuppgifter får ej lämnas inte ut till tredje part annat än om berörd person samtyckt till det eller om det är nödvändigt för att uppfylla våra förpliktelser enligt avtal eller lag.

I de fall vi lämnar ut personuppgifter till tredje part skall ett sekretessavtal upprättas som säkerställer att personuppgifterna behandlas på ett betryggande sätt.

Ecrucial överför inte personuppgifter i andra fall än de som uttryckligen anges i denna policy.

### **Vid misstanke om regelbrott**

GDPRs krav på skydd av personinformation innebär krav:

- Skydd av missbruk d.v.s. skydd mot missbruk av information som Ecrucial har tillgång till enligt lag, avtal eller medgivande.
- Skydd mot spridning av personinformation till icke behörig part  
Notera här specifikt konsekvenserna av att lagra information som Ecrucial äger och ansvarar för i miljöer som Ecrucial vare sig äger, ansvarar för eller har avtal runt.

I bägge fallen skall:

- Informationssäkerhetsansvarig samt VD kontaktas och informeras
- Informationen skall minst omfatta regelbrottets karaktär (vilken typ av regelbrott som t.ex. medvetet, omedvetet, brister i instruktioner eller teknik) samt omfattning.
- I samband med spridning av information till obehörig finns dessutom ett krav på anmälan till tillsynsmyndighet inom 72 timmar.

Notera i sammanhanget eventuella konsekvenser av en stulen laptop eller mail på publik eller annan PC.

## Referenser

Länk till regelverket:

[Datainspektionens version](#)

Samt

[EU-versionen på svenska](#)

Länk till interna Ecrucial dokument:

Organisation:

[GDPR-organisation hos Ecrucial](#)

Laglig grund:

[Sammanfattning av vad som räknas som laglig grund](#)

Allmän ordlista:

[Allmän ordlista för GDPR](#)

Samtyckes dokument:

[Folder för mallar med samtyckesdokument](#)

Detta dokument:

[Detta policydokument](#)

GDPR-dokument på Intranätet:

[GDPR-dokument på intranätet](#)

## Ansvar

Ecrucial Consulting Group AB är personuppgiftsansvarig, vilket innebär att vi är ansvariga för hur dina personuppgifter behandlas och att dina rättigheter tas tillvara.

Denna dag, 2018-10-02, har följande policy upprättats för Ecrucial Consulting Group AB.

Godkänt av:

Datum

---

---

---

Namnförtydligande och roll