**GDPR Policy**

**Systematiskt dataskyddsarbete**

**Mimers Vittjärv AB**

**2018/2019**

**Uppdaterad: 2018 08 09**

Innehåll

[1. Definitioner 2](#_Toc521661183)

[2. Lagliga grunder 2](#_Toc521661184)

[3. Principer vi följer 3](#_Toc521661185)

[4. Lagring 3](#_Toc521661186)

[5. Säkerhet 3](#_Toc521661187)

[6. Incidenter 3](#_Toc521661188)

[7. Rutiner 3](#_Toc521661189)

[7.1 Lagring 4](#_Toc521661190)

[7.2 Säkerhet 4](#_Toc521661191)

[7.3 Gallring 4](#_Toc521661192)

[7.4 Utlämning/Radering 4](#_Toc521661193)

[7.5 Incidenter 4](#_Toc521661194)

[8. Informationstexter 4](#_Toc521661195)

[9. Biträdesavtal 4](#_Toc521661196)

[10. Behandlingsregister 4](#_Toc521661197)

# Definitioner

GDPR är den nya europeiska lagstiftningen kring hanteringen av personuppgifter. Lagen ersätter den gamla personuppgiftslagen och hanteras av datorinspektionen, den stipulerar hur vi hanterar personuppgifter.

GDPR - General Data Protection Regulation

PU – Personuppgifter

Behandling – Allt man samlar, kategoriserar eller på annat vis hanterar avseende personuppgifter

LG – Laglig Grund. De lagliga grunderna för att behandla personuppgifter

GDPR gäller automatiserad behandling och manuell behandling som är sökbar i register

PUA – Personuppgiftsansvarig för verksamheten, ytterst ansvarig för att lagen efterlevs.

PU Biträde – Person som för bolagets räkning hanterar personuppgifter.

# Lagliga grunder

Samtycke. Om den registrerade har skriftligt *samtyckt* till behandlingen. Tex foton, överlämning av information.

Fullgöra avtal. Om du har (eller tänker skaffa) *ett avtal med den registrerade*. Tex anställningsavtal, hyresavtal mm. (Bara de uppgifter som är nödvändiga för avtalets ingående och uppfyllande får registreras).

Fullgöra rättslig förpliktelse. Om personuppgiftsansvarig har *en laglig skyldighet* att lagra informationen. Exempelvis bokföring, skollag, arbetsrätt, eller för att fastställa eller försvara rättsliga anspråk mm. Tex betyg, kränkningsärenden eller anställningsavtal.

Skydda grundläggande intressen. Om behandlingen är nödvändig för att ”*skydda intressen som är av avgörande betydelse för den registrerades eller andra fysiska personers liv*”. (Tex nödvärnsrätt som kan användas när den berörda personen själv inte kan lämna samtycke och behandlingen ändå är nödvändig.)

Myndighetsutövning och Allmänintresse. Om behandlingen är nödvändig ”*för att genomföra en uppgift av allmänt intresse*” eller som ”*ett led i den personuppgiftsansvariges myndighetsutövning*. Tex ”nödvändig registrering av personuppgifter i samband med naturkatastrofer” och ”registrering som är nödvändig för att en myndighet ska kunna sköta sina uppgifter”.

Intresseavvägning. Om den som bedriver verksamhet (eller en tredje part) har ”*ett berättigat intresse*” av att hantera personuppgifterna. Under vissa omständigheter är det då möjligt att göra en *intresseavvägning* som ger rätt att hantera personuppgifter utan samtycke, tex när flera personalansvariga inom en koncern behöver personuppgifterna.

# Principer vi följer

Det ska vara lagligt, korrekt och öppet.

Ändamålsbegränsning – vi har bara den information vi verkligen behöver.

Uppgiftsminimering – vi har så lite information som möjligt.

Lagringsminimering – vi spara så kort tid som möjligt.

Ansvarsskyldighet – Integritet och konfidentialitet gäller.

Vi behandlar enbart uppgifter med ett tydligt ändamål och syfte, i behandlingsregistret finns de olika kategorierna av behandlingar, med syftet och den lagliga grunden klarlagd.

Informationen ska enbart finnas för att den behövs, så länge som den behövs. Därefter ska den tas bort.

Alla anställda har ansvar att följa lagstiftning och principerna, ytterst ansvarig är PU Ansvarig.

# Lagring

Vi lagrar för närvarande på hårddiskar, med lösenord. Detta kommer under året att förändras och senast våren 2019 kommer all lagring att ske i ”moln”, tex Google Drive.

# Säkerhet

Vi avser att styra över både lagring och kommunikation till Google Drive. Alla datorer är lösenordsskyddade. Analog dokumentation sparas i låst dokumentskåp och låst dokumentrum.

# Incidenter

Incidenter anmäles omedelbart till PUA, som inom 72 timmar anmäler till datainspektionen.

# Rutiner

PU Ansvarig läsåret 2018/19 Tina Mörtberger, Inger Lundqvist.

PU Biträde läsåret 2018/19 MP Ekonomi.

### Lagring

All dokumentation ska lagras på Google Drive. PUA gör mappar där enbart de som behöver informationen har tillgång. Pappersdokument som behövs lagras i dokumentskåpet, nyckel tillgänglig för personal med behov av informationen. Dokument som bara måste finnas kvar (tex betyg för barn som slutat) lagras i dokumentrummet – dit har endast PUA tillgång till nyckel.

### Säkerhet

Lösenord på personliga arbetsdatorer, lärarkalendrar stannar på jobbet, ingen känslig information på mail (eller andra osäkra källor) – allt förmedlas i rätt Google Drive – grupp.

### Gallring

Den som lagrat informationen ansvarar för att den tas bort. Årligen görs en gallring av gammal information, personuppgiftsansvarig ansvarar för att så sker.

### Utlämning/Radering

Ska ske skyndsamt vid begäran.

### Incidenter

Anmäls till PUA omedelbart.

# Informationstexter

Till nya vårdnadshavare, personal och andra berörda skickar vi en kort informationstext om våra behandlingar av PU, via mail (eller pappersform om så krävs), med hänvisning till websidan. På websidan finns vår policy.

På personalsidorna på Google Drive finns en mapp där allt material finns tillgängligt.

# Biträdesavtal

Biträdesavtal finns med MP Ekonomi, ett original vardera hos Mimers Vittjärv AB och MP Ekonomi.

# Behandlingsregister

Behandlingsregistret finns i personalmappen på Google Drive, samt i rektors dator.