GDPR:

- General Data Protection Regulation.
- Ersätter PUL – Personuppgiftslagen.
- Träder i kraft den 25 maj 2018.

Vilka omfattas av GDPR?

- GDPR är en förordning, EU-lagstiftning.
- Gäller alla.
    - Företag.
    - Organisationer.
    - Myndigheter.
- Som behandlar personuppgifter rörande personer som vistas inom EU:s gränser.

Vad är en personuppgift?

Enligt GDPR:s definition:

- Varje upplysning som avser en identifierad eller ”identifierbar” fysisk person
    - Direkt
    - Indirekt
    - Genom kombination av uppgifter eller uteslutningsmetoden

Sanktioner:

- 2% av årsomsättningen på koncernnivå eller 10 miljoner EUR för mindre allvarliga överträdelser
- 4% eller 20 miljoner EUR för allvarligare fall
- Färre än 100 fall per år i Sverige
- 100-tusentals i andra EU-länder
- Datainspektionen är den myndighet som ska se till att dataskyddsförordningen följs

Definitioner:

- **Personuppgift:**
  - Varje upplysning som avser en identifierbar person.
- **Behandling:**
  - Läsa, skriva, vidarebefordra, radera, uppdatera osv.
- **Personuppgiftsansvarig:**
  - Alla företag som registrerar och behandlar personuppgifter.
- **Personuppgiftsbiträde:**
  - Alla företag som behandlar personuppgifter för den personuppgiftsansvarige.
- **Personuppgiftsincident:**
  - En säkerhetsincident som bryter mot lagstiftningen.

Vad innebär GDPR i praktiken?

- **Samtycke**

  Behöver vi samla in skriftligt om vi inte har laglig grund till personuppgiftshanteringen. Rättsliga skyldigheter, uppfylla avtal, intresseavvägning såsom bokföringslagen, anställnings-avtal, kollektivavtal, anhörigregister kräver inget samtycke. Däremot namn och bild på en webbsida kräver samtycke.

- **Rättning**

  Kandidaten har rätt att ändra sin persondata vi har lagrat.

- **Utdrag**

  Kandidaten har rätt att få se och begära ut den data vi lagrat.

- **Radering**

  Kandidaten har rätt att ta tillbaka samtycket och begära att vi raderar data.

- All data som lagras ska lagras med ett tydligt syfte och ändamål.
- Personuppgiftsansvarig, dvs vi, ska kunna fullgöra våra rättsliga skyldigheter.
- Får inte lagra data längre än nödvändigt för de ändamål de samlats in för.

Kunder:

- Vid upplägg av ny kund ska ni endast lägga in den information ni får från kunden för att dom ska godkänna vår faktura för betalning.
- Om vi fakturerar en privatperson får inte personnumret framgå på fakturan, men vi behöver personnumret i K2 för att kunna säkra upp kunden.
- Håller vi oss till ovanstående regler så är det okey att skicka fakturorna via mail.
- Idag har vi kundregister i både K2 och Visma Business. Det är i K2 som vi lägger upp kunden och denna information förs över till Visma Business med faktura filerna.
- Eftersom detta är bokföringsmaterial måste vi spara allt i 7 år i K2.

Leverantörer:

- Vi har ett leverantörsregister i Visma Business.
- När vi lägger upp en leverantör så använder vi oss av den informationen som står på fakturan och så länge vi gör det så behöver vi inte ändra vårt arbetssätt.
    - Namn
    - Adress
    - Organisationsnummer
    - Bankgiro/Bankkonto
- Eftersom detta är bokföringsmaterial måste vi spara allt i 7 år i Visma Business.
- Inom ISO-arbetet gör vi en leverantörsbedömning, dessa sparas i 2 år.

Vad har vi gjort?

- Kartlagt
  - Personuppgifter vi hanterar
  - Vilka som har tillgång till personuppgifterna – alla har fått skriva på ”Avtal om tystnadsplikt”
  - Var och hur länge dessa sparas
- Upprättat en Integritetspolicy & riktlinjer avseende GDPR
- Information
  - Till alla anställda & inhyrd personal via mail
  - Via vår webbsida
- Lönespecifikationer skickas via Kivra från och med juni
- Begärt in samtycken från dem som finns med på vår webbsida
- Skrivit avtal med våra Personuppgiftsbiträden