Riskhantering och personuppgiftslagen (PUL)

Swermas Risk Forum den 26 mars 2015

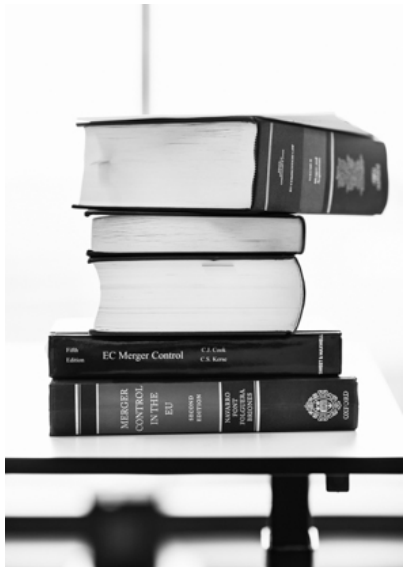
Erica Wiking Häger

Vilka är riskerna för ett företag som bryter mot PUL?

Vad är personuppgifter?

- *”all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet”*
- Exempel: namn, telefonnummer, IP-adresser, fotografier, ljudupptagningar, lokaliseringsuppgifter, kreditupplysningsinformation
- Extremt bred definition - även krypterad information kan vara personuppgifter

Vilka lagar och regler gäller?



EU:s dataskyddsdirektiv (95/46/EU)

- PUL
- Patientdatalagen
- Kameraövervakningslagen

Förslag till ny dataskyddsförordning

- Gemensamma regler inom EU
- Skärpta krav för företag
- Skärpta sanktioner: 5 % av global omsättning eller MEUR 100

Vad innebär de skärpta kraven i förslaget till ny förordning?

- Dokumentera användning av personuppgifter
- Krav på adekvat IT- och informationssäkerhet
- Utse ett personuppgiftsombud
- Genomför risk- och sårbarhetsanalyser för nya projekt
- ”Privacy by design”
- Rapportera dataintrång

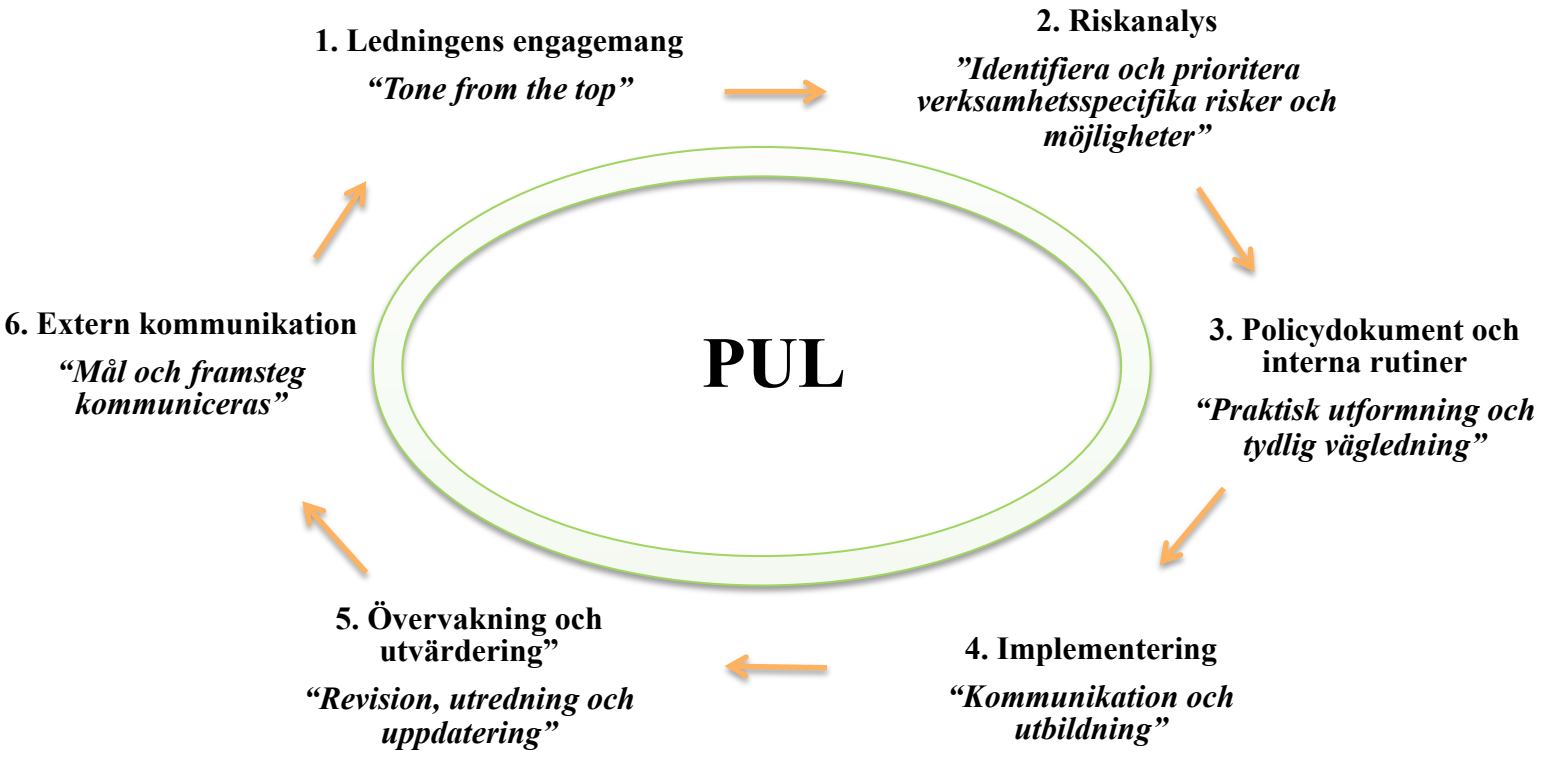
Vilka är riskerna?

- Tillsyn från myndigheter
- Sanktionsavgifter
- Böter eller fängelse
- Skadestånd
- Förlust av kunddata
- Goodwillskada
- Kundförluster
- Kostnader att utreda incidenter
- Tid och kraft från management

Hur kan ett företag hantera riskerna?

Compliance program

- Strukturerat arbete med PUL i bolag



Kontaktuppgifter

Erica Wiking Häger
Advokat, delägare, ordförande
Corporate Sustainability & Risk Management

Telefon: +46 8 595 063 30
Mobil: +46 709 777 330
E-post: ewh@msa.se