Torsdagen den 17 maj 2018

Advokat Fredrik Björklund och jur.kand. Dan Johansson

DATASKYDDSFÖRORDNINGEN (GDPR)

– VAD BEHÖVER MAN TÄNKA PÅ?

CRUSNER
ADVOKATBYRÅ

Vad är GDPR?

En lag man måste följa för att få behandla personuppgifter

Vad är då **nytt** med GDPR? Bl.a.:

- **Hårdare krav** för att få behandla personuppgifter
- **Större skyldigheter** gentemot registrerade
- **Högre böter och skadestånd**
- Större krav på **dokumentation och avtal**

CRUSNER
ADVOKATBYRÅ

När får man behandla personuppgifter?

Man får BARA behandla personuppgifter om:

1. Man har fått **samtycke** från personen
2. Man har ett **avtal** med personen
3. Man är **tvungen enligt lag** att behandla personuppgiften
4. Man har ett **berättigat intresse** att behandla personuppgiften

5. Man utför myndighetsutövning eller agerar i allmänt intresse
6. Man skyddar grundläggande intressen

*Man måste **veta** vilka som är ens godkända anledningar (=lagliga grunder)*

CRUSNER
ADVOKATBYRÅ

Behandling av personuppgifter

”Behandling” och ”Personuppgift”

– Två ord som betyder *väldigt mycket*

Personuppgift: *Alla* uppgifter man kan använda för att identifiera en människa

Behandling: *All* slags användning,

– från insamling till gallring

(kom ihåg att även lagring är behandling)

CRUSNER
ADVOKATBYRÅ

Behandling av personuppgifter

Behandling + Personuppgift = GDPR

Tänk brett! Exempel:

- Man läser ett mail
- Man skriver ett brev
- Man antecknar en kunds namn i en lista
- Man lämnar ut ett telefonnummer
- Man hämtar in anställdas hälsouppgifter … med mera

Man måste ha (minst) en laglig grund för att göra detta

CRUSNER
ADVOKATBYRÅ

När man ska vara *extra* försiktig

Var försiktig med dessa personuppgifter:

- Uppgifter om mer ”avlägsna” personer (t.ex. anställdas anhöriga)
- Känsliga uppgifter (hälsa, ras, politisk åskådning etc.)
- Mindre nödvändiga uppgifter
- Gamla uppgifter

GDPR:s principer för behandling (art. 5) ska styra all behandling
– ändamålsbegränsning, uppgiftsminimering
och lagringsminimering m.m.

CRUSNER
ADVOKATBYRÅ

Gamla personuppgifter

Hur ska man göra sig av med personuppgifter?

- Ofta det svåraste praktiska problemet?

En anställd slutar, ett kundförhållande upphör, man byter leverantör etc.

  - har man då en godkänd anledning att behålla personuppgifter om dessa?

- Måste man radera alla personuppgifter?
- I så fall när?

Olika bedömningar i olika fall

T.ex. personuppgifter om kund ska som utgångspunkt raderas ett år efter att kundavtal upphört

CRUSNER
ADVOKATBYRÅ

Rätten att bli glömd m.m.

<u>Man har omfattande skyldigheter gentemot den registrerade</u>

- Den som är registrerad har i många fall ”*rätt att bli glömd*”
  - Man kan t.ex. alltid kräva att få slippa direktmarknadsföring
- Man kan också kräva att ens personuppgifter är korrekta
- Man kan också begära att få information om bl.a. hur ens personuppgifter behandlas
- Man har rätt att begära skadestånd hos Datainspektionen

CRUSNER
ADVOKATBYRÅ

Ansvarsfördelningen – personuppgiftsansvarig och personuppgiftsbiträde

- **Personuppgiftsansvarig**
  - Den som *bestämmer* över behandlingen
- **Personuppgiftsbiträde**
  - Den som behandlar personuppgifter för personuppgiftsansvarigs räkning

  Några regler för biträdet:

  - *Allmänt lämplighetskrav*: personuppgiftsansvarig måste anlita ett personuppgiftsbiträde som kan garantera att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas
  - Det måste finnas ett *avtal* (personuppgiftsbiträdesavtal)

CRUSNER
ADVOKATBYRÅ

Vad ska man då göra?

Ingen kan följa GDPR i minsta detalj

- Mycket lär handla om att ha **rutiner** för sin behandling
  - Bl.a. när och hur man gallrar
- Man måste veta **varför** man behandlar personuppgifter
- Man måste upprätta vissa **avtal** och andra dokument
- **Säkerheten** är central
- Viktigt att kunna **visa** att man följer GDPR

CRUSNER
ADVOKATBYRÅ

Vanliga brister

- Gallring sker inte i tid och rutiner saknas
- Man lämnar ut felaktig information och rutiner saknas
- Otillräcklig säkerhet och rutiner saknas
- Register saknas
- Personuppgiftsbiträdesavtal saknas

CRUSNER
ADVOKATBYRÅ

Att tänka på efter denna föreläsning

Man bör eller måste upprätta bl.a. dessa handlingar. Det rekommenderas att man anlitar juridisk hjälp med åtminstone vissa av dessa dokument.

- **Internt policydokument** (med rutiner ang. gallring, säkerhet m.m.)
- **Registerförteckning** (register över behandlingen av uppgifter)
- **Informationsförteckning** (som ska lämnas ut till registrerade)
- **Avtal** (personuppgiftsbiträdesavtal)

Viktigt även för att få en överblick över hur man behandlar personuppgifter!

CRUSNER
ADVOKATBYRÅ

Att tänka på efter denna föreläsning

Ställ er dessa frågor. Gör ni det, besvarar frågorna och upprättar dokumenten i föregående slide har ni kommit en bra bit på vägen!

- Vilka personuppgifter behandlar vi?
- Varför behandlar vi dem?
- Vilken är vår lagliga grund för behandlingen (se slide 3)?
- Hur behandlar vi personuppgifterna – vad gör vi med dem?
- Vad har vi för olika system, register och avtal (mail, telefoner, lönesystem etc)?
- Med vilka delar vi personuppgifter?
- Hur får vi behandlingen av personuppgifter säker?
- Hur gallrar vi och begränsar omfattningen av personuppgifter?

CRUSNER
ADVOKATBYRÅ

För vidare kontakt

fredrik.bjorklund@crusner.se

dan.johansson@crusner.se

william.wangberg@crusner.se

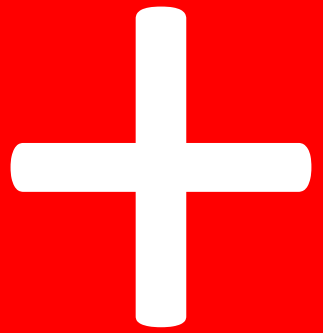
CRUSNER
ADVOKATBYRÅ

DocuWare

Fredrik Lövgren

IT-HÄLSOKONTROLL

- Genomgång av alla IT-system
  - Servermiljö, nätverk, E-mail, säkerhet, backuper m.m.
  - Risker och säkerhetsbrister
  - Flaskhalsar
- Genomgång av IT-relaterade avtal
  - Bredband
  - Print
  - Telefoni
  - Licenser för Microsoft, Apple och Adobe m fl.
  - Backup- och antiviruslicenser
- GDPR
  - Pulsmätning av er GDPR-förberedelse
- Fullständig dokumentation
- Rekommendationer



halsokontroll@docuware.se

docuware.se/it-halsokontroll

IT är en funktion som skall stödja kärnverksamheten att nå sin fulla potential. Det innefattar en stabil och säker miljö samt rätt system och verktyg för att kunna arbeta effektivt.

IT-hälsokontroll - helt kostnadsfri

Vi erbjuder en hälsokontroll av er nuvarande IT-miljö, helt utan kostnad.

Resultatet av genomförd kontroll är:

- en fullständig dokumentation av hur IT-miljön ser ut idag.
- pulsmätning på ert behov av åtgärder inför GDPR.
- slutsatser och rekommendationer till förbättringar.

Dokumentationen ger er ett värde oavsett vilken IT-partner ni väljer att samarbeta med framöver.

För oss är förståelsen för kunden och relationen grundläggande och vi vill därför investera denna tid i att lära känna er och er verksamhet

Hur går det till?

Vi kommer till er arbetsplats under en halvdag. Det enda vi behöver av er är att någon är på plats och ger oss tillgång till rätt information.

Vi går bl a igenom följande:

- Servermiljö (servrar, OS-versioner, funktioner)
- Nätverk och säkerhet
- Backuper och redundans
- Datorer (Uppdateringar, programversioner, antivirus)
- Hantering av personuppgifter (GDPR)
- IT-relaterade avtal (t ex telefoni, nätverk)
- Identifiering av flaskhalsar, problem och risker

Vad händer sedan?

Efter IT-hälsokontrollen kommer vi att dokumentera och analysera nuläget, samt sammanställa våra rekommendationer på förbättringsområden, effektivisering och digitalisering.

Slutligen kommer vi att besöka er igen för att presentera rapporten. Vi går tillsammans igenom innehåll, slutsatser och rekommendationer.

Kontakta oss för mer information.

halsokontroll@docuware.se

www.docuware.se/it-halsokontroll

010 211 53 00

Docu:Ware IT

Docu:Ware

CRUSNER
ADVOKATBYRÅ