Personuppgiftsincidenter - Incidenthantering

Agnes Hammarstrand & Erica Thore, 18 september 2023

Vilka är vi?

- Agnes Hammarstrand och Erica Thore, Advokatfirman Delphi
- Delphi är en progressiv affärsjuridisk advokatbyrå med erkända specialister inom de flesta av affärsjuridikens områden
- Stort team specialister inom GDPR, tech och IT-juridik

Delphi

BG Institute

Delphi

Agenda

- Introduktion och översikt
- Vad är en personuppgiftsincident?
- När ska en personuppgiftsincident anmälas?
- Hur anmäla?
- Information till individer
- Praktiska tips, exempel och frågestund

Introduktion och översikt

BG Institute

Reglerna om incidenter i GDPR

- GDPR – skydd för integriteten
- Personuppgifter tolkas brett
- Incidentreglerna - del i de allmänna reglerna om hög säkerhet vid behandling av personuppgifter
- Flera olika skäl att ha koll på reglerna
  - Hand i hand med gott infosäk-arbete
  - Ej badwill
  - Risk för böter upp till EUR 10 000 000 eller 2% av totala globala årsomsättningen

Art 33 - anmälan (skäl 73, 85, 86, 87 och 88)

Art 34 – information

(skäl 73, 86, 87 och 88)

BG Institute

Delphi

Andra krav på anmälningar

NIS-lagen

Krav anmäla incidenter **utan onödigt dröjsmål** till MSB

Gäller för samhällsviktiga och digitala tjänster

Utökat omfång genom NIS 2

Säkerhetsskyddslagen

Krav anmäla IT-incidenter **skyndsamt** till säkerhetspolisen i vissa fall, bl.a. om

- ”skäl att anta att en säkerhetsskyddsklassificerad uppgift” otillåtet kan ha röjts
- systemet har betydelse för säkerhetskänslig verksamhet och incidenten allvarligt kan påverka säkerheten i systemet

BG Institute

Delphi

Incidentreglerna i korthet

BG Institute

Delphi

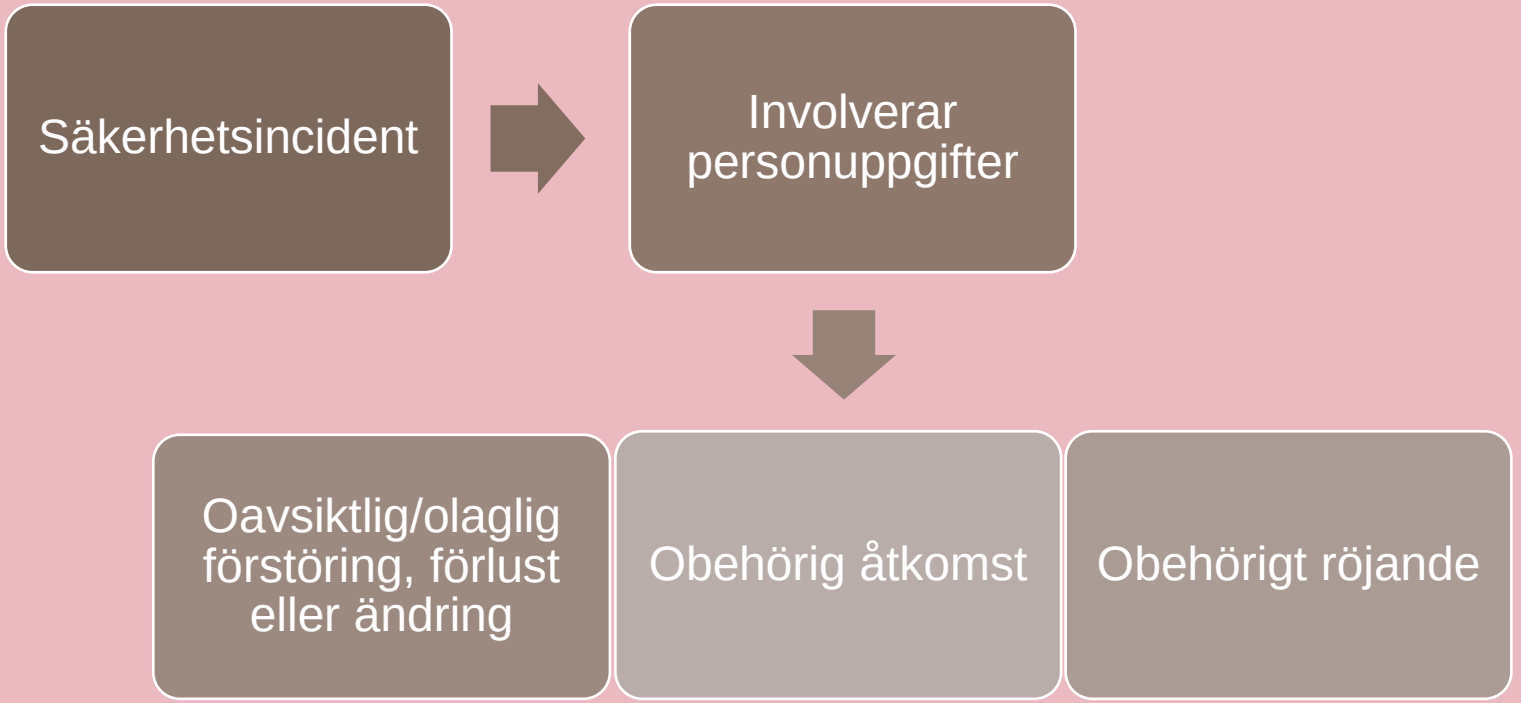
Viktiga vägledningar

- EDPB
  - Guidelines 9/2022 on personal data breach notification under GDPR
  - Riktlinjer 01/2021 om exempel på anmälan av personuppgiftsincidenter
- IMY
  - Information om personuppgiftsincidenter

Vad är en personuppgiftsincident?

Vad är en personuppgiftsincident?

- En säkerhetsincident – som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till personuppgifter



Olika typer av personuppgiftsincidenter

”Konfidentialitetsincident”	”Integritetsincident"	"Tillgänglighetsincident"
Obehörigt eller oavsiktligt röjande av, eller åtkomst till personuppgifter	*Obehörig eller oavsiktlig ändring av personuppgifter*	*Obehörig eller oavsiktlig förlust av, åtkomst till, eller förstöring av personuppgifter*

BG Institute

Delphi

Exempel på vad som INTE är en incident

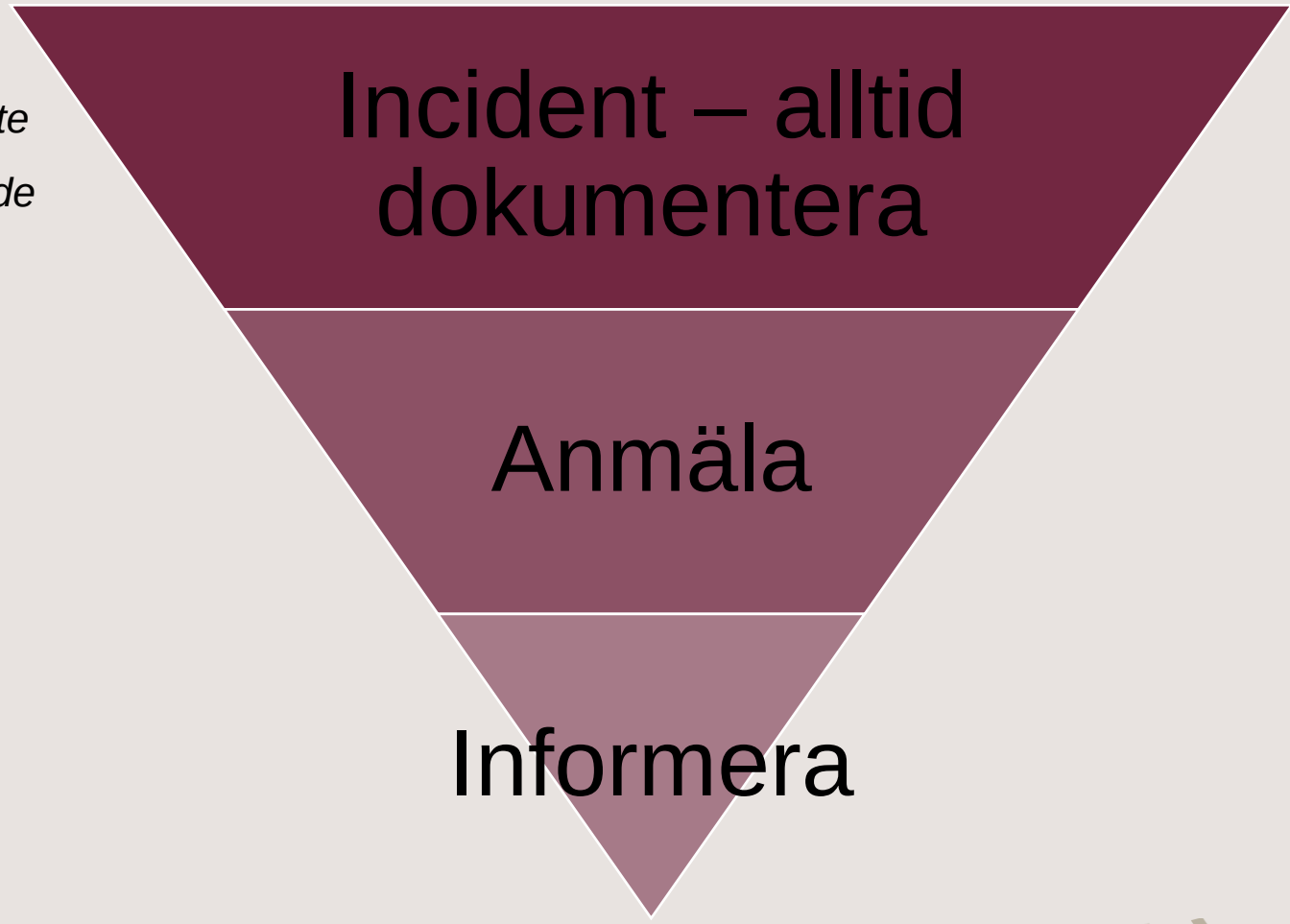
- Planerat systemunderhåll
- Behandling av uppgifter vi inte fick behandla – är inte personuppgiftsincident men bryter mot andra regler enligt GDPR

När ska en incident anmälas?

BG Institute

När anmäla?

- Om en personuppgiftsincident skett, om det *inte är osannolikt att incidenten medför en risk för de registrerade*
- *Utan onödigt dröjsmål* och senast inom 72 timmar från att personuppgiftsansvarige **fått vetskap**



När har personuppgiftsansvarig vetskap?

- ”Rimligt säker”
- Beror på omständigheterna i det enskilda fallet
- Om misstanke men inte vetskap:
  - Möjlighet att göra kort undersökning (räknas ej med i tid)
  - Skyldighet att agera snabbt vid misstanke
- OBS! Den ansvarige måste ha rutiner för att snabbt skaffa sig vetskap! Oklart hur långt kravet går…

BG Institute

Delphi

Exempel när vetskap

Redan vid förlust av enhet (oavsett om enheten kanske hittas senare)

Vid tidpunkt då vet om intrång

Utomstående informerar om åtkomst (oavsett om inte sett något)

När information från personuppgiftsbiträde

BG Institute

Delphi

När osannolikt att incident medför risk?

- Tolkas restriktivt – hög tröskel
- Riskbedömning i det enskilda fallet
  - Hur stor är den potentiella skadan?
  - Hur sannolikt är det att denna skada inträffar?

Undantag

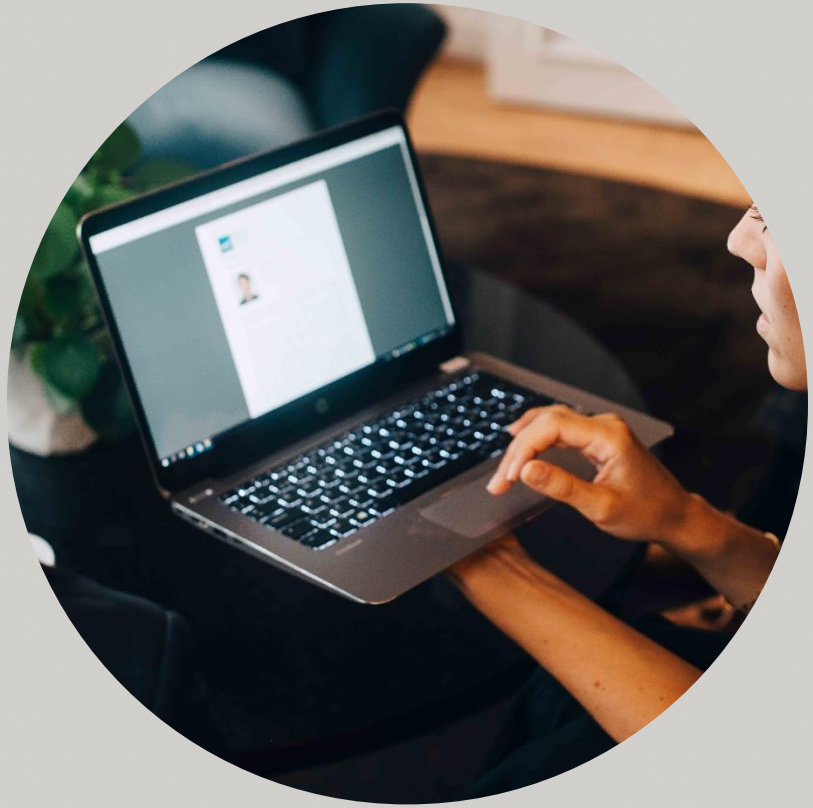
- Redan offentliggjorda uppgifter
- Oläsbara uppgifter
  - Exempel om Uppgifterna är krypterade och krypteringsnyckeln är intakt
  - Krävs bra kryptering ”state of the art”
  - I vissa fall kan incidenten ändå behöva anmälas
    - T.ex. om inte är tillgänliga

BG Institute

Delphi

Även om inte anmäla: Dokumentera!

- Så komplett dokumentation över incidenten som möjligt, bl.a.
  - Omständigheterna kring personuppgiftsincidenten
  - Incidentens effekter
  - De korrigerande åtgärder som vidtagits
- Dokumentationen ska göra det möjligt för IMY att kontrollera efterlevnaden



BG Institute

Delphi

För sent?

- Skälen för förseningen ska anges
- Kort försening kan anses ok om giltiga skäl och ej sätts i system
- Vid mer komplexa personuppgiftsincidenter kan informationen lämnas i omgångar
- Möjlighet att ”samla ihop” flera incidenter till en anmälan
  - Om likheter mellan incidenterna
  - Om det skett inom en begränsad period

Biträdets roll

- Skyldighet att underrätta ansvarig
- Omedelbar information från biträde till ansvarig, när biträde får kännedom om personuppgiftsincidenten, kan utgöra riskreducerande faktor
- Biträdet behöver inte avgöra sannolikheten av att personuppgiftsincidenten medför en risk innan biträdet underrättar ansvarig
- Om biträde tillhandahåller sina tjänster till flera ansvariga som påverkas av personuppgiftsincidenten måste samtliga underrättas

Hur anmäla?

Hur anmäla till myndigheten?

- Anmälan skickas in till IMY (om ansvarig tillsynsmyndighet)
- Anmälan och komplettering kan bl.a. göras genom E-formulär

Informationskrav till tillsynsmyndigheten

Personuppgiftsincidentens art, kategorier av och det ungefärliga antalet personuppgifter och registrerade som berörs

Namn och kontaktuppgifter på dataskyddsombud eller andra kontaktpunkter

Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten

Beskrivning av de åtgärder som den ansvarige har vidtagit eller föreslagit för att åtgärda incidenten

Att tänka på

- Var ärlig
- Överväg hur du formulerar dig
- Utgångspunkt: offentlighet
- Ansökan kan (SKA) kompletteras om information saknas
- Var förberedd, ha t.ex. standardtexter redo
- Alla personuppgiftsincidenter, dess effekter och åtgärderna som vidtagits ska dokumenteras
- Intern utredning – ha frågor förberedda och rutiner

BG Institute

Delphi

Gränsöverskridande incidenter

- En incident med anknytning till flera medlemsstater är *gränsöverskridande*
- Anknytning till flera medlemsstater om:
  - personuppgiftsincidenten påverkar behandlingar som äger rum inom ramen för verksamhet i flera EU-länder; eller
  - personuppgiftsincidenten påverkar registrerade i väsentlig grad/kommer sannolikt i väsentlig grad påverka registrerade i mer än ett EU-land.

BG Institute

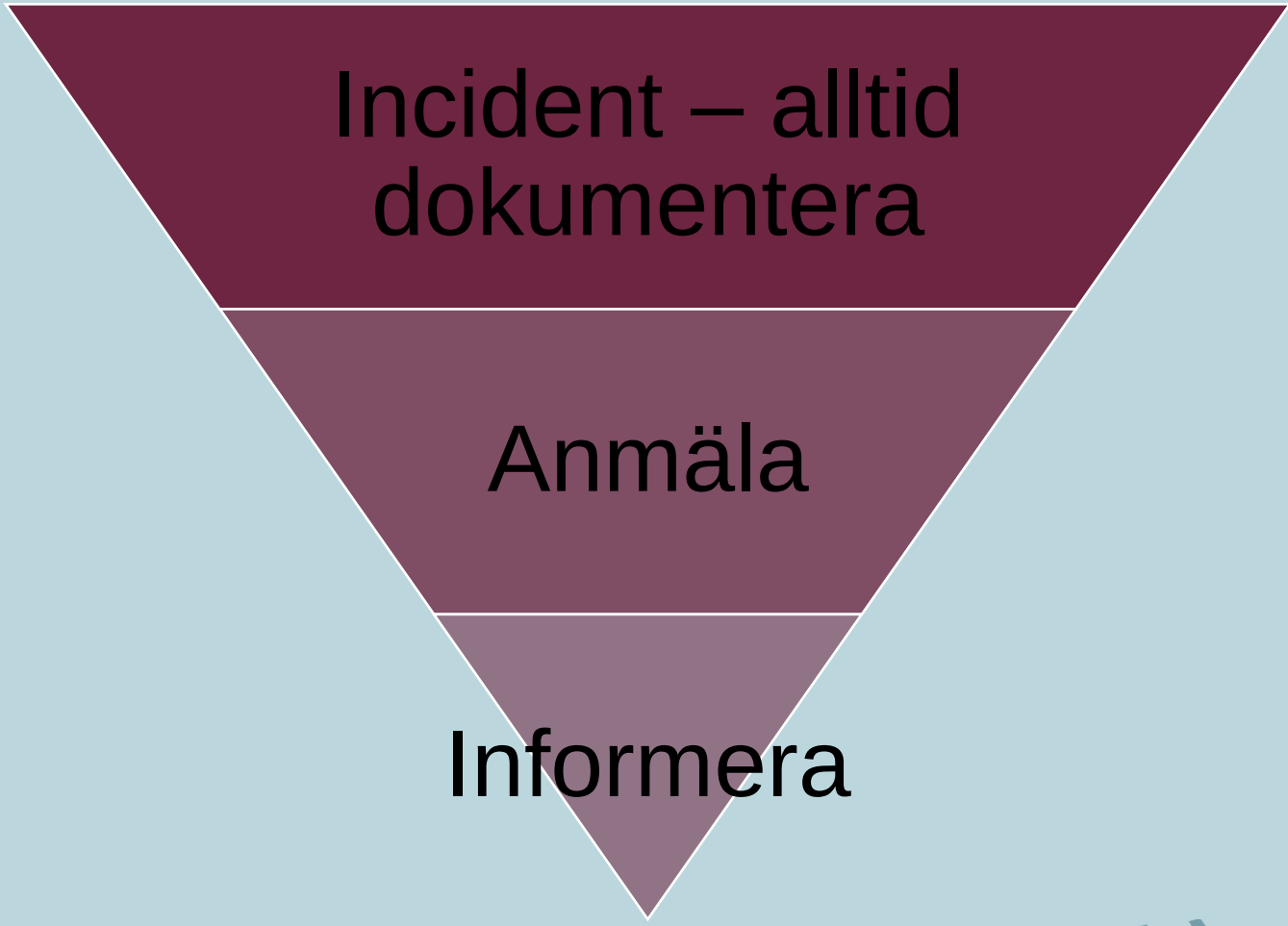
Delphi

Information till individer

BG Institute

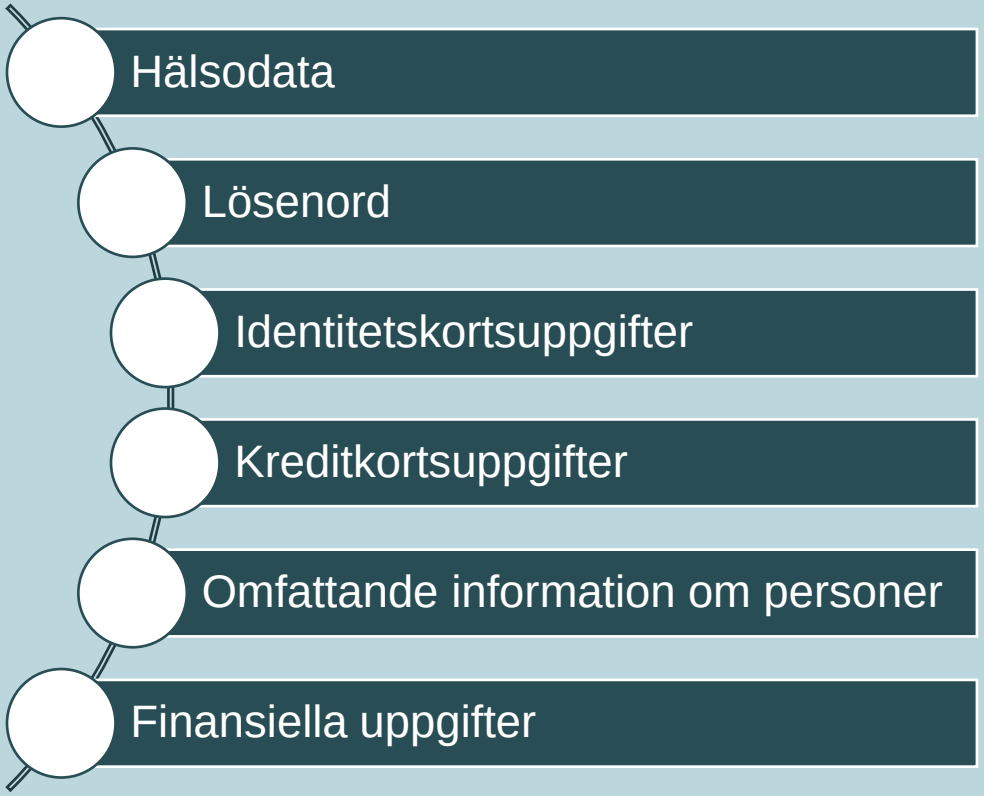
Information till de registrerade

- Information ska ges vid **hög risk** för fysiska personers rättigheter och friheter
- Syfte – registrerad ska kunna vidta åtgärder
- I exceptionella fall kan information till registrerade behöva ske före anmälan till IMY



När hög risk för fysiska personer?

- Fysiska, materiella eller immateriella skador för enskild
- Hänsyn till sannolikhet och svårighetsgrad
- Sannolikhet att någon integritetsskada sker



BG Institute

Delphi

Undantag

- Lämpliga tekniska och organisatoriska åtgärder – kryptering
- Oproportionerlig ansträngning – tolkas restriktivt
- Om information inte kan ges till registrerade krävs ibland att information ges offentligt

Hur informera?

- Krav enligt lag på informationen – OBS!
- Hur ska de registrerade kontaktas?
  - Dedikerade meddelanden, inte tillsammans med nyhetsbrev etc.
  - E-post, sms, website banners, post, annonser i media
  - Flera kommunikationssätt
  - Så individerna förstår (språk)

BG Institute

Delphi

Praktiska tips

BG Institute

Praktiska tips

- ✓ Gott säkerhetsarbete är A och O - ta fram incidenthanteringsplan
- ✓ Utbilda personal. Alla behöver känna till att incidenter ska anmälas
- ✓ Ha ett team för incidenter som hanterar detta praktiskt och bemanningsschema. Detta team behöver ha högre kunskap
- ✓ Var förberedd.
  - ✓ Öva – ha en rutin framme.
  - ✓ Ta fram mallar och FAQ, t.ex. för information till individer
- ✓ Panel för andra kompetenser, t.ex. tekniker, PR, osv.
- ✓ Försäkring?

BG Institute

Delphi

Praktiska tips

Specifika områden

- ✓ Identifiera känsliga områden
  - Om ransomware händer – vad är mest känsligt?
  - Om exfiltrering sker – vad skulle vara mest känsligt?
- ✓ Identifiera troliga åtgärder som kommer behöva vidtas
  - Information till berörda parter – var finns adresser – vilka ska vi kontakta?
- ✓ Se över säkerheten på identifierade känsliga områden
- ✓ Hantera biträden och partners – avtala och kom överens om en rutin. Vem gör vad ,osv?

BG Institute

Delphi

Exempel Case

- 1177-incidenten (bl.a. DI-2019-3375)
  - Sanktionsavgift
- Trygg-Hansa (DI-2021-1905)
  - Sanktionsavgift
- V-klass (IMY-2022-9092)
  - Reprimand och föreläggande

BG Institute

Delphi

Frågestund

Agnes Hammarstrand

Advokat / Partner

Mobil: +46 730 83 50 70
E-mail: agnes.hammarstrand@delphi.se

Erica Thore

Associate

Mobil: +46 709 25 25 64
E-mail: erica.thore@delphi.se

Delphi

Personuppgiftsincidenter i praktiken – hur hanteras de juridiskt?

Agnes Hammarstrand & Erica Thore, Stockholm den 7 februari 2024

Till dig som deltog på dagens webbinarium erbjuder vi nu 20 % rabatt på vår uppföljningskurs

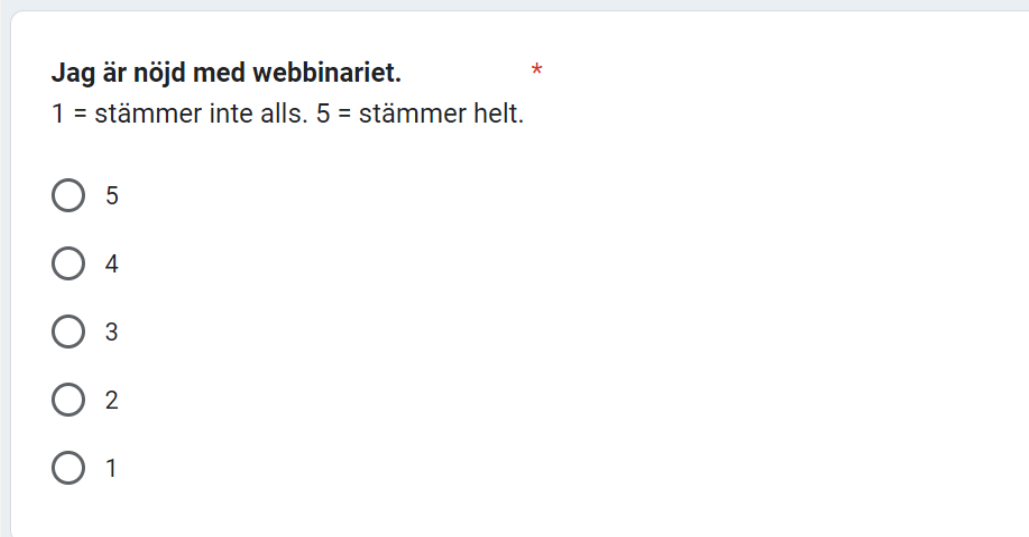
Boka din plats senast den 22 september för att ta del av erbjudandet

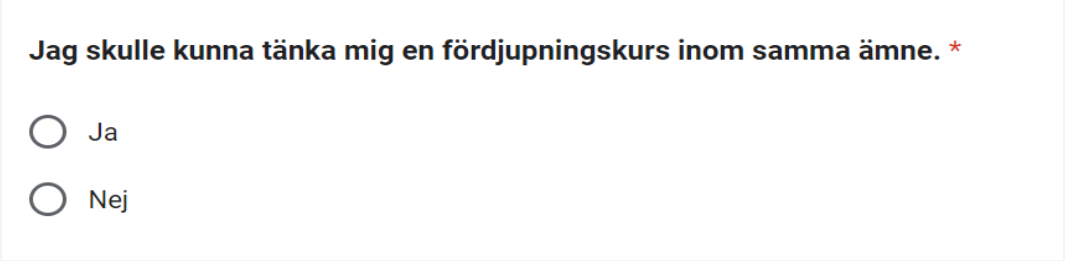
Använd rabattkod: **webb20**

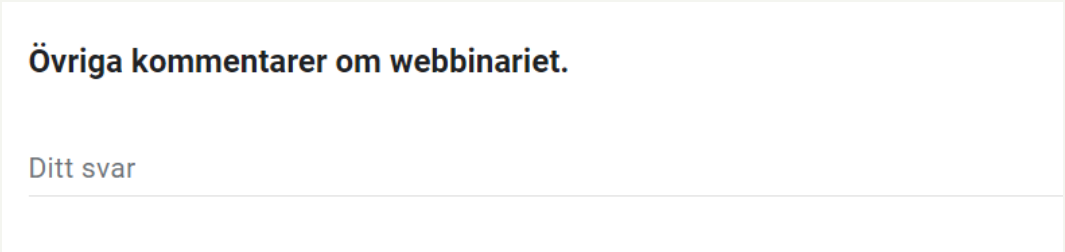
BG Institute

Låt oss veta vad du tycker!

Vi skulle uppskatta om du tog 30 sekunder till att fylla i vår kursutvärdering







Länk till utvärderingen finner du i chatten.

BG Institute

Tack för att ni lyssnat!

Har du några frågor? Kontakta oss på marknad@bginstitute.se.

BG Institute

Delphi

/ We love challenges