Har din virksomhed styr på persondata og datasikkerhed?

Corporate Counsel Academy | September 2014

Advokat, partner Janne Glæsel, jgl@gorrissenfederspiel.com
Advokat Tue Goldschmieding, tgg@gorrissenfederspiel.com

Agenda

Agenda

1. Status på Persondataforordningen

2. Hvordan får man styr på compliance og datasikkerhed i praksis?

Status på Persondataforordningen

Status – Persondata reformen

22. januar 2012: Viviane Reding

”The new rules will help business in three ways. Firstly they create legal certainty. Secondly, they simplify the regulatory environment. Thirdly, they provide clear rules for international transfers”

25. januar 2012: Kommissionens forslag til en Persondataforordning

Modernisering

Styrke individets rettigheder (retten til at blive glemt. Lettere adgang til egne data, kontrol med egne data og større transparens)

Reducerer administrative tiltag – anmeldelser afskaffes

Undtagelser for SME’s (ingen anmeldelser, krav på gebyr ifb. indsigt, ingen Data Protection Officer, ingen krav om ”Impact Assessment/PIA - risikoanalyse)

Fremme uniformitet og regelsammenhæng i EU - grundrettigheder respekteres

Status – Persondata reformen

21. oktober 2013

Parlamentet - LIBE Komiteens vedtagelse af et mandat til at starte forhandlinger med Rådet mhp. at opnå enighed om reformen før valget i maj 2014

Offentliggørelse af "Consolidated draft of the Regulation" – skærpelse – bl.a. i relation til samtykke indenfor forskningsområdet, bevisbyrde, sanktioner mfl.

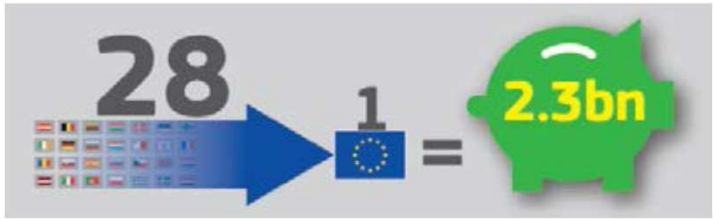
12. marts 2014

"The European Parliament today cemented the strong support previously given at committee level to the European commission's data protection reform …. by voting in plenary with 621 votes in favour, 10 against and 22 abstentions for the Regulation and 371 votes in favour, 276 against and 30 abstentions for the Directive). The reports of MEPs Jan-Philipp Albrecht and Dimitrios Droutsas, on which members of the European Parliament voted, are a strong endorsement of the commission's data protection reform and an important signal of progress in the legislative procedure…."

Status – Persondata reformen

Parlamentet

Opbakning til ”the architecture and the fundamental principles”



One continent, one law

One-stop-shop – main establishment

The same rules for all companies - regardless of their establishment

“Data protection is about your fundamental right to privacy”

Status – Persondata reformen

Ikrafttræden 2 år efter vedtagelse næppe før 2017/18

Fortsat uenighed, særlig om

- Direktiv contra Forordning – Parlamentet › Forordning – DK m.fl. ›Direktiv
- One-stop-shop
- Om offentlige myndigheder skal være omfattet

"Next meeting of Justice Ministers on the data protection reform will take place in June 2014"

Italien har overtaget EU formandskab for 2. halvår 2014 efter Grækenland – Intet nyt!

Status – Persondata reformen

Geografisk afgrænsning – Art 3

Gælder ikke kun dataansvarlige og databehandlere i EU også for sådanne uden for EU

- Hvis behandling vedrører udbud af varer og tjenesteydelser
- Overvågning/tracking af personer i EU
- Også uanset betaling eller ej

Status – Persondata reformen

Definition af persondata – Art 4

"'Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, genetic, mental, economic, cultural or social or gender identity of that person."

Status – Persondata reformen

Særlige kategorier af personoplysninger – Art 9

Forbud mod behandling af bl.a. helbredsoplysninger med mindre

- Samtykke
- Vital interesse
- Egen offentliggørelse
- Nødvendig af hensyn til den offentlige interesse
- Hvis betingelser i Art 83 er opfyldt – samtykke m.fl.

Kommission – delegerede retsakter

Status – Persondata reformen

Data portabilitet– Art 15

Lettere adgang til egne data

Individets ret til sletning af personlige oplysninger – Art 17

Sletning egne data (fra servere, UGC platforme, øvrige platforme)

Retten til at blive glemt er modificeret – tredjemand skal kun informeres om sletning af links, hvis offentliggørelsen har været uberettiget, men

EU Domstolens afgørelser i Google sagen og om Logningsdirektivet ……..

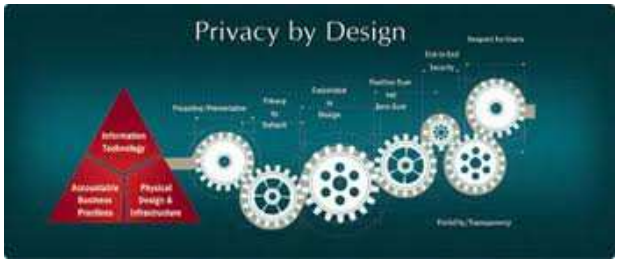
Profilering – Art 20

Begrænsninger

Status – Persondata reformen

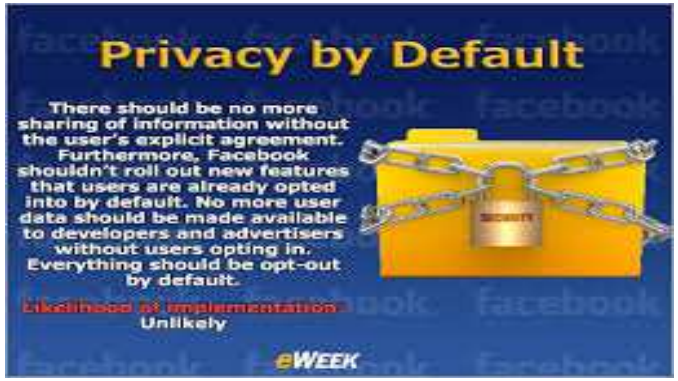
Privacy by design – Art 23

Data beskyttelse skal indtænkes fra start i produkter og services



Privacy by default – Art 23

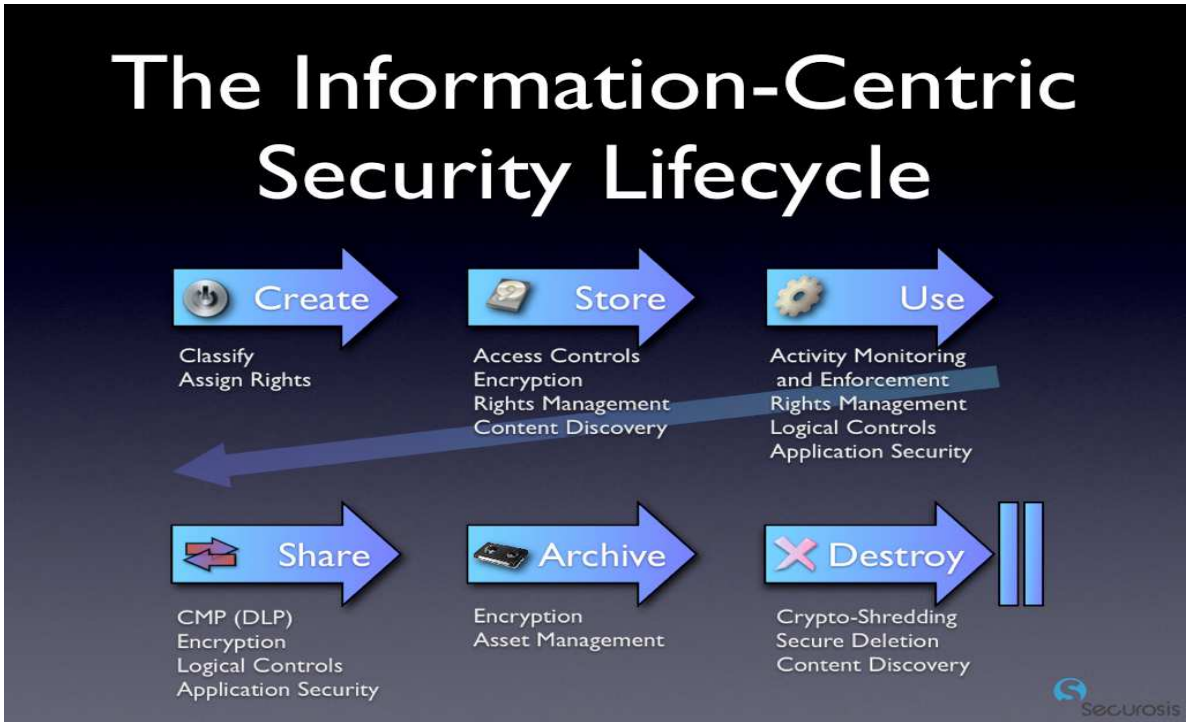
Default settings skal have den mest databeskyttelsesvenlige indstilling



Status – Persondata reformen

Datasikkerhed – Art 30

- Sikkerhedspolitik
- Uddannelse, guidelines
- Sikkerhedsforanstaltninger - fysisk som systemmæssigt
- ICO's guidance on data security breach management



Status – Persondata reformen

Notificering ved sikkerhedsbrud – Art 31-32

Til myndighed

Til datasubjekt - retten til at vide hvornår ens oplysninger er blevet hacket

Status – Persondata reformen

Data Protection Officer – Art 35-37

Virksomheder med 250 ansatte og derover eller hvis hovedformål er databehandling

Certificeringsmulighed

Status – Persondata reformen

Overførsel til tredjelande – Art 41-44

- Krav om ”adequate level of protection”
  - Binding Corporate Rules
  - Standard Clauses
  - Contractual Clause
  - EU Kommissionens beslutning
- Styrkelse af Safe Harbour – 13 forslag
- European Data Protection Board

One-stop-shop – Art 54

- Hvis virksomheden opererer i flere EU-lande – ”Main establishment”
- Personer har klageadgang til lokale DPOs/Tilsyn

Status – Persondata reformen

Sanktioner – Art 53 og 79

Stærke sanktionsbeføjelser for myndighederne

Bøde op til 100 mio. Euro eller 5% (3% højere end Kommunionens forslag) af den årlige Worldwide omsætning (alt efter hvad der er størst)

Hvordan får man styr på compliance og datasikkerhed i praksis?

Fokus på datasikkerhed

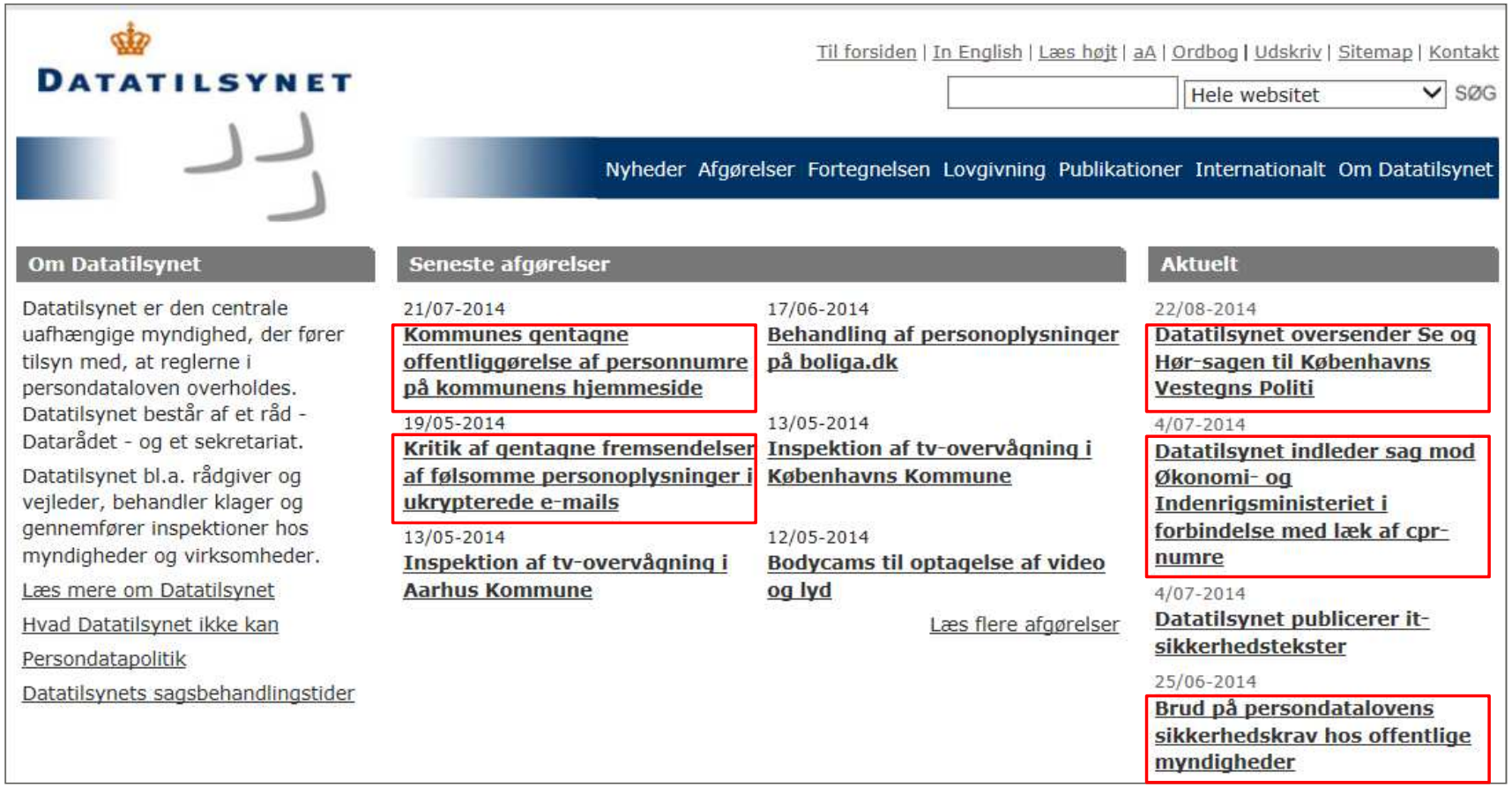
»CSC-sagen rokker ved den grundlæggende tillid«

Eksperter: IBMs system burde have opdaget tys-tys-klilde

Danmarks største hackersag

Nets bekræfter: Medarbejdere har fri adgang til data

Fokus på datasikkerhed



Hvor går det galt?

Internt i organisationen

Politik og retningslinjer

- Utilstrækkelig beskrivelse af samt undervisning i sikkerhedsprocedure i forbindelse med persondatabehandling – eksempelvis brug og deling af personoplysninger.
- Manglende fokus på overholdelse af de persondataretlige regler i forbindelse med udvikling og markedsføring af nye produkter og ydelser.

Teknisk sikkerhed

- Manglende kontrol med sikkerhedsforanstaltninger truffet hos databehandlere.
- Ubegrænset adgang til oplysninger – dvs. oplysninger kan tilgås ud over hvad der er nødvendigt for rolle eller funktion.

Manglende halvårlig kontrol af medarbejderes autorisationer.

Brug af anonyme bruger-id'er (testbrugere eller fællesbrugere), hvorved tilgang og anvendelse af personoplysninger ikke kan spores til én fysisk person.

Manglende stikprøvekontrol af log.

Hvor går det galt?

Menneskelige fejl

Offentliggørelse af fortrolige eller følsomme oplysninger på internettet

- som følge af fejl eller uvidenhed om, hvad der må offentliggøres, eller
- som følge af utilstrækkelig anonymisering mv.

Fejl eller uvidenhed i forbindelse med udsendelse af e-mails,

F.eks. at der sendes til forkert adresse, at fortrolige eller følsomme personoplysninger sendes i ukrypteret e-mail via internettet, eller at flere modtagere af en e-mail angives i modtagerfeltet (i en situation, hvor de ikke bør kende hinandens oplysninger).

Uvedkommende dokumenter bliver blandet ind i et system

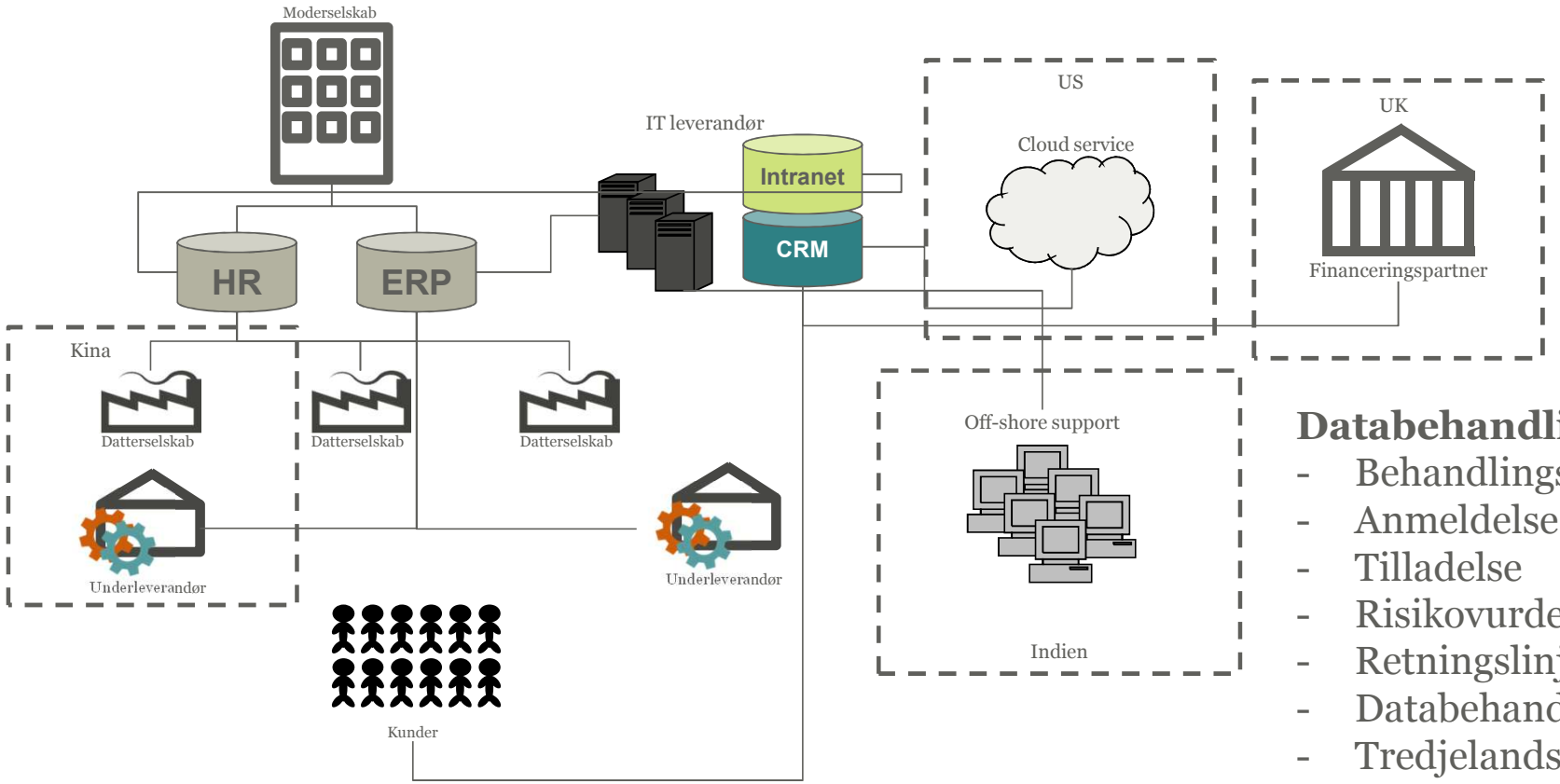
F.eks. i forbindelse med udskrivning og/eller afsendelse (ses både ved elektronisk og manuel post).

Hvor går det galt?

Utilstrækkelige eller fejlbehæftede it-løsninger

- Manglende kryptering af formularer på hjemmesider til brug for fremsendelse af fortrolige eller følsomme oplysninger.
- Utilstrækkelig adgangsløsning i forbindelse med adgang via internettet til at se eller indtaste bl.a. følsomme oplysninger.
- Adgang til for brugeren uvedkommende oplysninger som følge af fejl i it-systemet
- Manglende kontrol med afviste adgangsforsøg.
- Manglende logning eller problemer med, om de loggede oplysninger kan anvendes til at spore, hvilke oplysninger en medarbejder har tilgået.
- Uhensigtsmæssig brug af administratorrolle i forbindelse med IT-systemer

Mapping af databehandling og overførsler?



Databehandling:

- Behandlingshjemmel
- Anmeldelse
- Tilladelse
- Risikovurdering
- Retningslinjer og uddannelse
- Databehandlingsaftale
- Tredjelandsoverførselsaftale

Risikoanalyse

Risikoanalyse

Risk Assessment Report

ID	Risk description	Impact	Probability	Risk Assessment Score	Regulatory requirement	Security measures and Risk Controls	Risk Control Assessment	Risk Control Score	Mitigating Action
	Repair department								
1	Repair modtager i forbindelse med reklamation returnerede medier, som kan være lagret med kundernes personlige data. Disse data kan være af ret følsom karakter. Der kan være en risiko for, at medarbejderne samt tredjemand (eksempelvis i tilfælde af, at nye (returnerede) medier videresælges til en ny tredjemand) får uberettiget kendskab til disse data. Dette kan medføre væsentlige dårlig omtale i medier og på sociale tjenester.	3	2	6	Sikkerhedsbekendtgørelsen§ 9; I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes de fornødne foranstaltninger for at sikre, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.	Der gives kun mundtlige instrukser til medarbejderne om, at der skal slettes, når medierne modtages. Der er ikke udarbejdet retningslinjer på området.	4	24	For at sikre at uklarheder omkring håndteringen ikke forekommer, anbefales det, at der udarbejdes interne skriftlige retningslinier/arbejdsbeskrivelse til medarbejderne vedrørende modtagelse af returnerede medier ved reklamation, herunder krav om sletning af medierne mv. for at sikre, at kundernes personlige data på medierne ikke videregives uberettiget. Der kan eventuelt indarbejdes en rapportering i processerne, når mediet er nulstillet.

Eksempel på en konsekvensanalyse

Risikoanalyse – Art 32-34

Data protection impact assessment (PIA/DPIA)

Konsekvensanalyse (PIA)

1) Beskrivelse af systemet:

- Skal give et omfattende og fyldestgørende billede af det samlede system
- Fx visualisering af design, snitflader og informationsstrømme

2) Identifikation af relevante risici

- Identificere omstændigheder, som vil kunne true eller kompromittere personlige data
- Vurdering af sandsynligheden for risiciene

Eksempel på en konsekvensanalyse

Konsekvensanalyse (PIA)

3) Identifikation af nuværende og foreslåede kontroller:

- Kontroller af enten teknisk eller ikke-teknisk karakter
- Tekniske kontroller kan være indbygget i systemet gennem design og konfiguration
- Ikke-tekniske kontroller er styrings- og driftsmæssige kontroller

4) Dokumentation af dækning og udestående risici

- Resultaterne af risikovurderingen dokumenteres i en PIA rapport

Kontakt os

Kontakt os

Janne Glæsel
jgl@gorrissenfederspiel.com
D +45 33 41 42 81
M +45 27 80 40 10

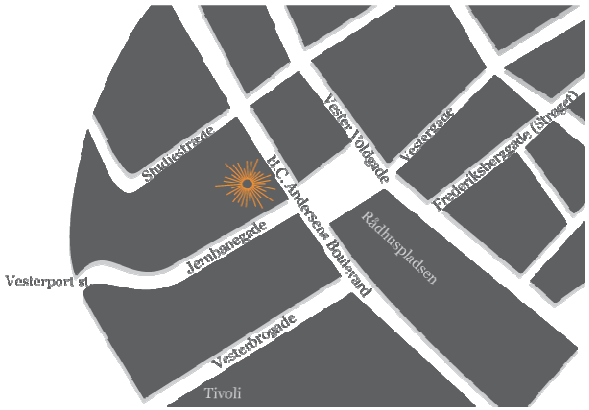
Tue Goldschmieding
tgg@gorrissenfederspiel.com
D +45 33 41 42 03
M +45 24 28 68 75

Find os

København

H.C. Andersens Boulevard 12
1553 Copenhagen V
Denmark

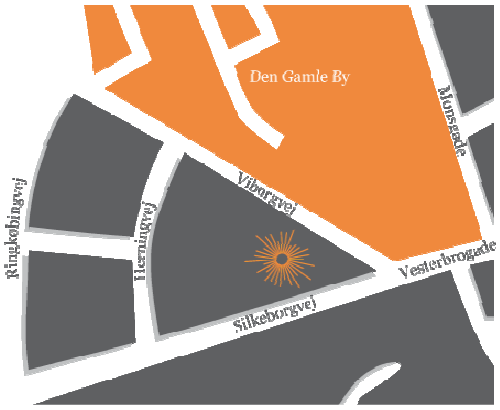
T +45 33 41 41 41
F +45 33 41 41 33



Aarhus

Silkeborgvej 2
8000 Aarhus C
Denmark

T +45 86 20 75 00
F +45 86 20 75 99



Online

www.gorrissenfederspiel.com
contact@gorrissenfederspiel.com