Når Compliance Bliver Kultur

ISO27001, ISAE 3402/3000 & EU GDPR – i teori og praksis

Siscon & HeroBase – 17. Januar 2019

AGENDA

- KORT OM SISCON & HEROBASE
- KRAV, STANDARDER OG LOVGIVNING – ET SAMSPIL
- HEROBASE'S UDGANGSPUNKT
- GØR DIT COMPLIANCE ARBEJDE SAMMENHÆNGENDE
- FORANKRING I FORRETNINGEN
- KULTUR & GEVINSTER

OM SISCON & HEROBASE

SISCON
... styrker din position

- Dansk konsulenthus og softwareleverandør siden 2004
- ControlManager™ skaber fundamentet virksomhedens ISMS / Complianceprogram
- Konsulentydelser – der matcher og udnytter ControlManagers™ potentiale
- Mere end 130 kunder i Danmark og Norge
- Kontor i Allerød med kursusfaciliteter
  18 medarbejdere – i en virksomhed i vækst

BØRSEN. GAZELLE 2017

BØRSEN. GAZELLE 2018

OM SISCON & HEROBASE

Hero

SISCON
... styrker din position

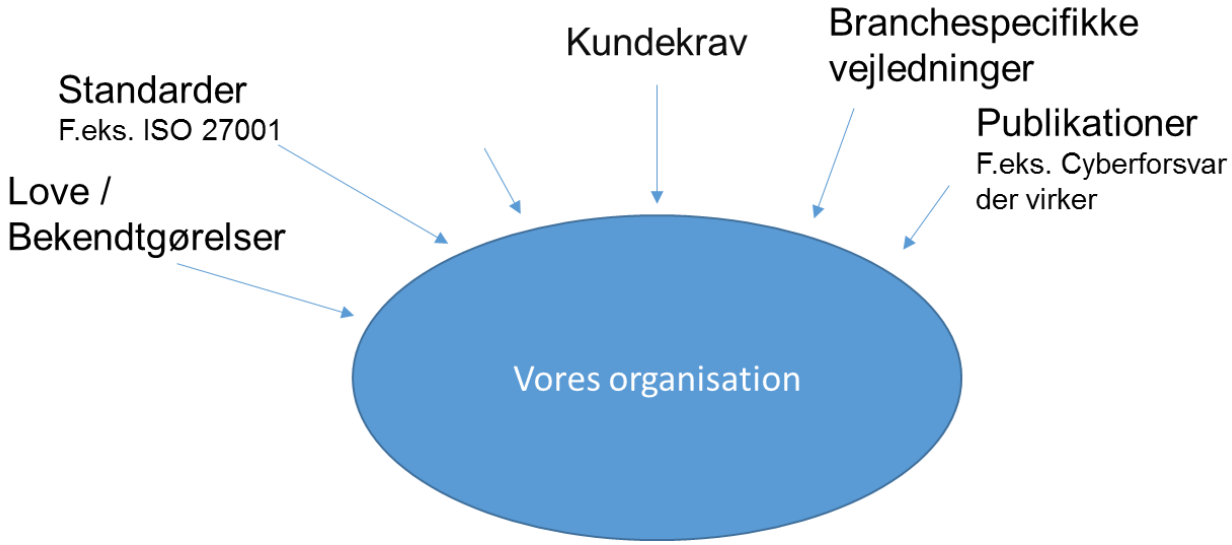
- Dansk IT-virksomhed med base i Søborg – 30 mand, 10 år
- Leverer kontaktcentersoftware – komplette løsninger til kontaktcentre inkl. backoffice
- SaaS løsninger inden for Outbound, Inbound og Markt. Automation (digitalisering, integrationer)
- Mere end 140 kunder i Danmark, Norden og beslægtede lande
- ”Every day there is a chance to do something extraordinary”

PRES FRA ALLE I ORGANISATIONEN

GDPR PROJEKTETS AFLEVERING?

UDFORDRINGEN

- ORGANISATIONER HAR MANGE FORSKELLIGE EKSTERNE KRAV DE SKAL VÆRE COMPLIANT MED
  - Ekstern lovgivning
  - Krav om brug af (branche)standarder
  - Krav fra kunder/leverandører
- MANGE KRAV ER HELT/DELVIST OVERLAPPENDE
- DET ER SVÆRT AT VURDERE
  - Hvem gør hvad internt for at sikre compliance?
  - Hvor er der overlap i krav?
  - Hvilke af vores interne tiltag understøtter eksterne krav?



Persondataforordningen er ”blot” endnu en række krav

I PRAKSIS – EU-GDPR EKSEMPEL

- EU-GDPR AFDELING 3 BERIGTIGELSE OG SLETNING
  - Art. 17, stk. 1 (a), (b), (c), (d), (e), (f)

- DATASUBJEKTET HAR RET TIL AT FÅ SLETTET PERSONDATA OM SIG SELV UDEN UNØDIG FORSINKELSE, OG DEN DATAANSVARLIGE HAR PLIGT TIL AT **SLETTE PERSONOPLYSNINGER UDEN UNØDIG FORSINKELSE**, HVIS DATA IKKE LÆNGERE ER NØDVENDIGE I FORHOLD TIL FORMÅLET ELLER,
- DATASUBJEKTET **TRÆKKER SIT SAMTYKKE TILBAGE** ELLER GØR INDSIGELSE ELLER MODSÆTTER SIG DATABEHANDLINGEN,
- SAMT I TILFÆLDE, HVOR DATABEHANDLINGEN ER ULOVLIG, ELLER SKAL SLETTES SOM FØLGE AF LOVGIVNING
- ELLER ANGÅR INDHENTNING AF PERSONDATA OM BØRN TIL BRUG I INFORMATIONSTJENESTER.

MAPNING AF EU-GDPR -> REGEL -> KONTROL - BÅDE GDPR OG TEKNISK OG ORG. KONTROLLER

EU-GDPR

DATASUBJEKTET HAR RET TIL AT FÅ SLETTET PERSONDATA OM SIG SELV UDEN UNØDIG FORSINKELSE, OG DEN DATAANSVARLIGE HAR PLIGT TIL AT **SLETTE PERSONOPLYSNINGER** UDEN UNØDIG FORSINKELSE, HVIS DATA **ER IKKE LÆNGERE NØDVENDIGE** I FORHOLD TIL FORMÅLET ELLER,

Regel

Regel

Regel

PROCESEJER ER ANSVARLIG FOR LØBENDE AT OPDATERE PROCESOVERBLIKKET MED BESKRIVELSER AF HVILKE DATA DER BLIVER BEHANDLET I DERES RESPEKTIVE PROCESSER, OG HVOR DISSE FLYDER HEN

Hvordan/detaljer

ISO 27001/2

9. 2. 5. Gennemgang af brugeradgangsrettigheder
Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder.

Regel

Systemejeren er ansvarlig for, med udgangspunkt i oversigt fra Brugeradministration, at gennemgå alle brugernes adgangsrettigheder, for deres respektive systemer, hver 3. måned.

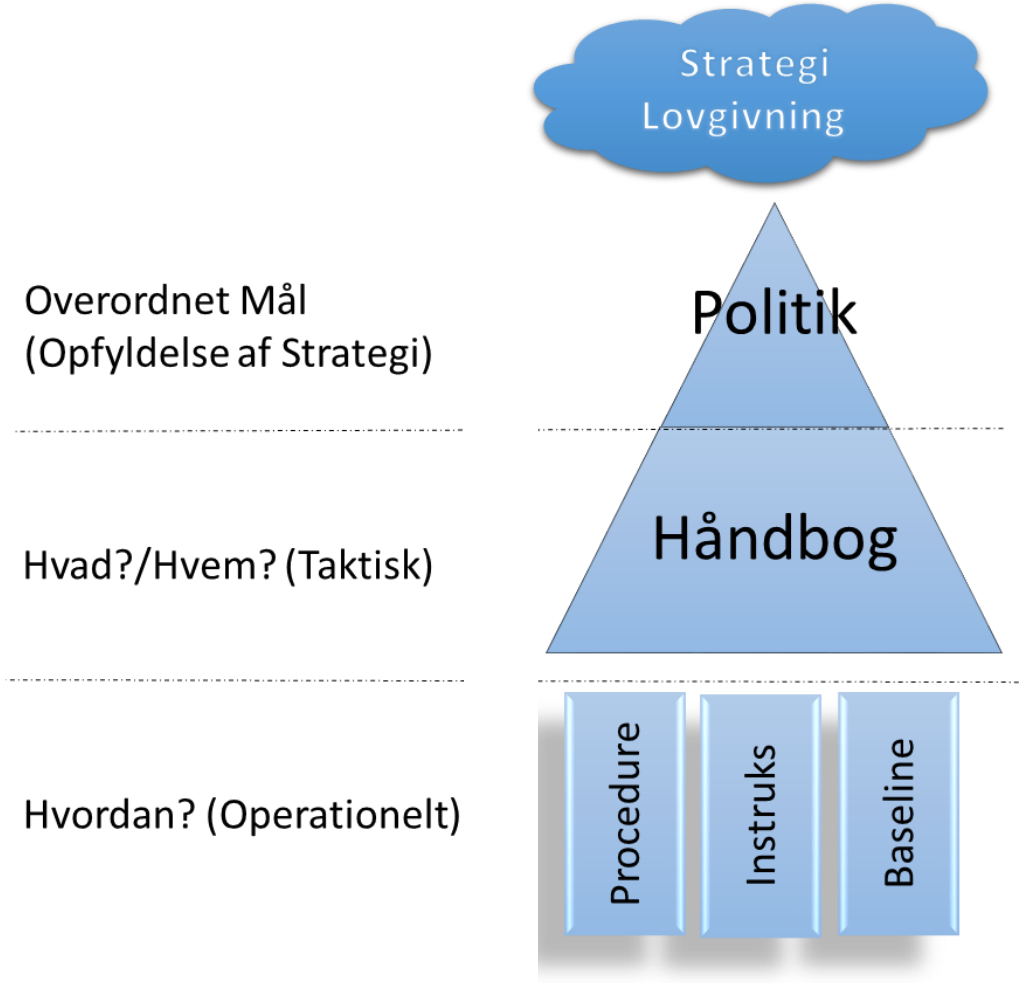
Hvordan/detaljer

RESULTAT = HÅNDBOG

- STRUKTURERET UDARBEJDELSE AF REGELSÆT ENDER UD I EN HÅNDBOG

- HÅNDBOGEN SIKRER:
  - Klare rammer for arbejdet
  - **Rolle- og ansvarsmodel**
  - Sikringstiltag
  - En ”rød tråd” fra krav til tiltag

VISHED FOR AT VI HAR STYR PÅ ALLE FACETTER AF EU-GDPR



FRA PAPIRCOMPLIANCE -> FAKTUEL COMPLIANCE

Hero SISCON ... styrker din position

3. 6. Artikel 17 – Ret til sletning (»retten til at blive glemt«)

3. 6. 1. stk. 1 (a), (b), (c), (d), (e), (f) ✔

Den dataansvarlige skal på datasubjektet anmodning og uden unødig forsinkelse slette persondata om datasubjektet, hvis:
- data ikke længere er nødvendige i forhold til formålet
- datasubjektet trækker sit samtykke tilbage
- gør indsigelse eller modsætter sig databehandlingen
- databehandlingen er ulovlig
- data skal slettes som følge af lovgivning
- angår indhentning af persondata om børn til brug i informationstjenester

”Krav jeg er underlagt”

Indirekte:

7. 1. 1. Fortegnelse over informationsaktiver

It-chefen har ansvar for, at alle it-aktiver bliver identificeret.

7. 1. 2. Fortegnelse over informationsaktiver

It-sikkerhedskoordinatoren sikrer at, der føres en fortegnelse over alle væsentlige it-aktiver, og at denne fortegnelse ajourføres løbende.

7. 1. 5. System til procesoverblik

Chefen for arkitekturafdelingen er ansvarlig for, at der til enhver tid, er etableret et system til at understøtte procesoverblikket for virksomhed X, hvori det er muligt at illustrere virksomhedens processer med tilhørende dataflows.

7. 1. 6. Opdatering af procesoverblik

Procesejer er ansvarlig for løbende at opdatere deres respektive procesoverblik med beskrivelser af, hvilke data der bliver anvendt i deres respektive processer, og hvor disse flyder hen

7. 1. 7. Kontrol af procesoverblik

Procesejer er ansvarlig for kvartalsvist at gennemløbe deres procesbeskrivelser samt flow og vurdere:

- Er der sket ændringer i mine behandling af data?
- Modtager/afgiver jeg andre data end de registrerede?
- Er der sket ændringer i hvor længe data er tilgængelige?

Egne regler – ”Hvad betyder det for mig?”

Skærmbillede fra ControlManager™

HEROBASE'S UDGANGSPUNKT – BÅDE KRAV OG EFTERSPØRGSEL

4. 7. Artikel 30 - Fortegnelser over behandlingsaktiviteter

4. 7. 1. stk. 1, (a), (b), (c), (e), (f) og (g) og stk. 3

Den dataansvarlige skal dokumentere sine behandlingsaktiviteter. Den skriftlige eller elektroniske dokumentation skal omfatte:
- navn og kontaktoplysninger
- herunder også på evt. repræsentant og databeskyttelsesrådgiver
- behandlingens formål
- kategorier af datasubjekter
- kategorier af persondata
- kategorier af modtagere, som dataene videregives til
- overførsel til tredjelande
- tidsfrister for sletning
- en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger.

4. 7. 2. stk. 4

Den dataansvarlige og databehandleren skal stille fortegnelserne skal stilles til rådighed for Datatilsynet efter anmodning.

4. 8. Artikel 31 - Samarbejde med tilsynsmyndigheden

4. 8. 1. stk. 1

Den dataansvarlige og databehandleren skal samarbejde om at imødekomme Datatilsynets anmodninger.

4. 9. Artikel 32 - Behandlingssikkerhed

4. 9. 1. stk. 1

Den dataansvarlige og databehandleren skal gennemføre passende te
databehandlingens risici for datasubjektet. I fastlæggelsen af risici og si
- det aktuelle tekniske niveau
- implementeringsomkostninger,
- databehandlingens karakter og omfang, dens sammenhæng og form
- risikoen for at påvirke personers rettigheder og friheder, herunder dere

4. 9. 2. stk. 1 (a), (b), (c) og (d)

Den dataansvarlige og databehandlerens vurdering af sikkerhedsnive
- pseudonymisering og kryptering af persondata
- sikring af fortrolighed, integritet, tilgængelighed
- behandlingssystemer og
- tjenesters robusthed
- rettidig genoprettelse af tilgængelighed
- adgang til persondata efter fysisk eller teknisk hændelse
- procedurer for regelmæssig afprøvning, vurdering og evaluering af si

4. 9. 3. stk. 2

Den dataansvarlige og databehandleren skal foretage en vurdering af

Vi vil gerne bede om lidt udførlig information om:

- Organisering af informationssikkerhed
- Personalesikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud og –hændelser

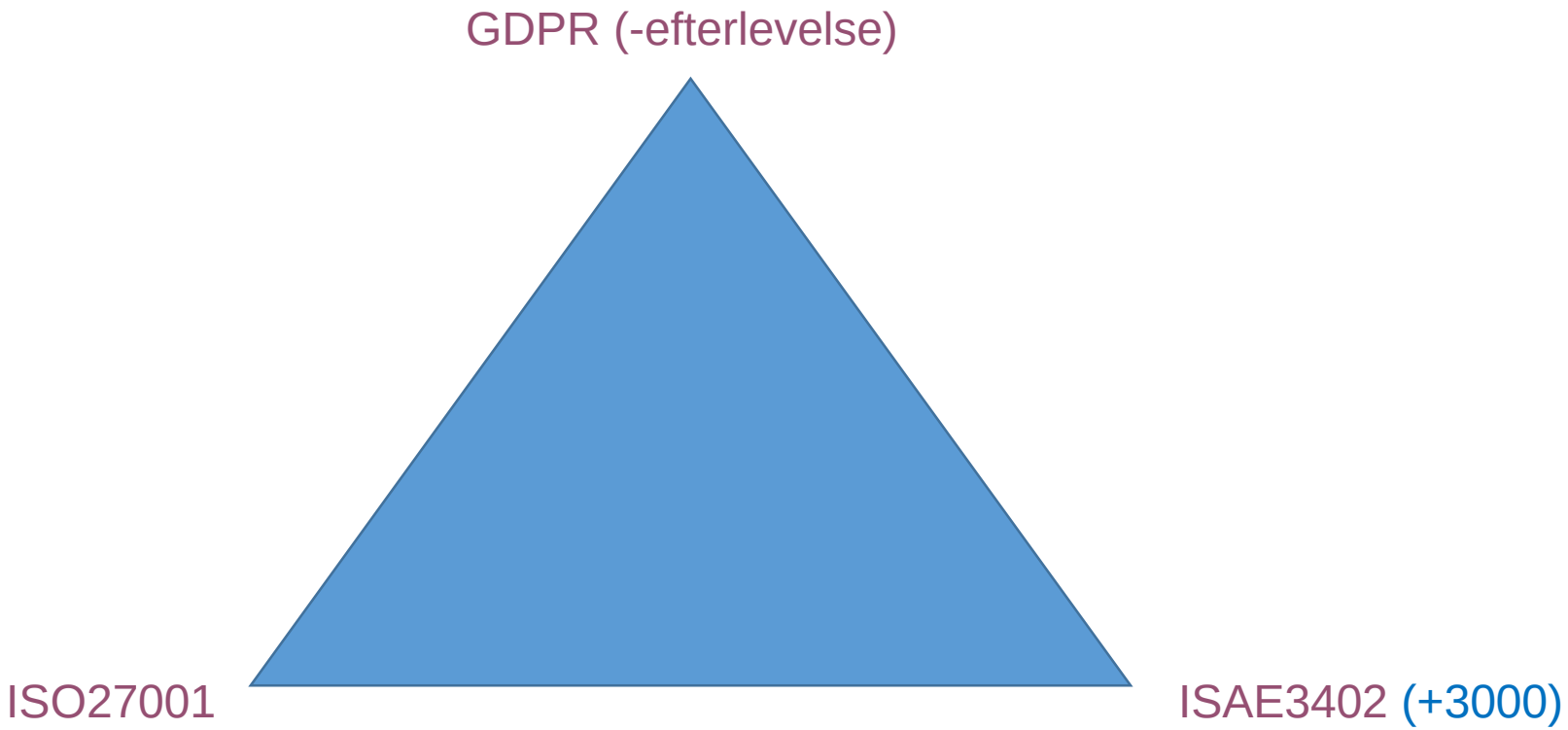
…og så bare lige lidt om hvordan I sikrer disse forhold løbende, og hvordan I dokumenterer det – naturligvis.

DEN FAMØSE 25. MAJ – OG KOBLING MED KUNDEBEHOV

- EU-GDPR AFDELING 4 DATAANSVARLIG & DATABEHANDLER
  - Art. 28, stk. 1

- DEN DATAANSVARLIGE MÅ UDELUKKENDE BENYTTE DATABEHANDLERE, DER KAN DOKUMENTERE TILSTRÆKKELIG GARANTI FOR, AT PASSENDE TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER ER IMPLEMENTERET.

SAMMENHÆNGEN I PRAKSIS



SAMMENHÆNGEN I PRAKSIS – SYNERGIER MELLEM ISAE 3402 OG 3000

ISAE3402 (type I)

Formålet med denne beskrivelse er at levere information til HeroBases kunder og deres interessenter (herunder revisorer) vedrørende kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE3402.

Beskrivelsen har herudover det formål at give information om vores informationssikkerhedsregelsæt, procedurer og kontroller, som er gældende for vores leverance af produktet og ydelsen Hero Outbound til vores kunder.

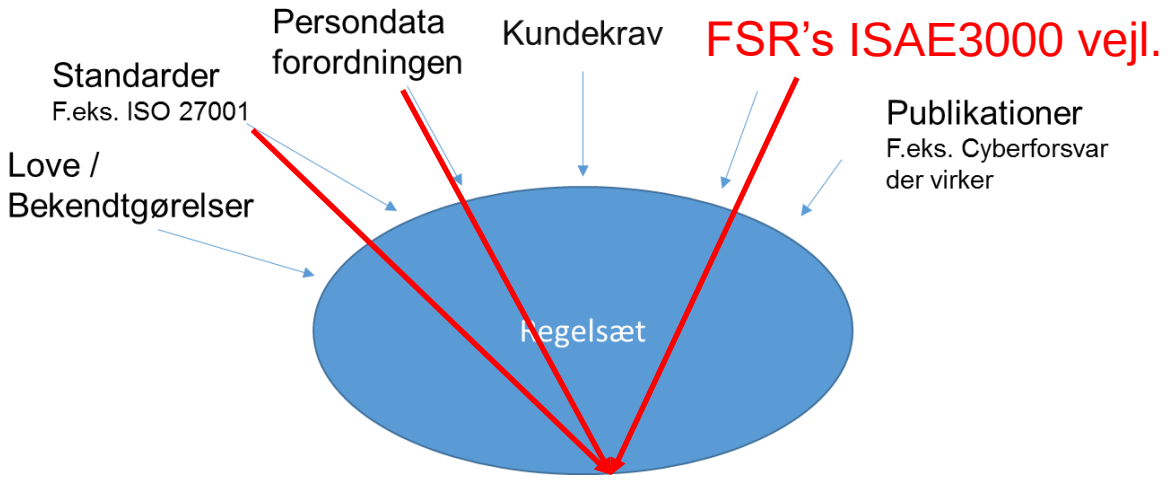
Art. 32 = ISAE 3402 (+ ISO 27001/2)

ISAE 3000

Formålet med denne beskrivelse er at levere information til HeroBases kunder og deres interessenter (herunder revisorer) vedrørende kravene og indholdet i databeskyttelses-forordningen (”GDPR”), beskrevet ud fra rammerne givet i den internationale revisionsstandard ISAE3000, herunder også standarden for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE3402.

Beskrivelsen har herudover det formål at give specifik information om forhold vedrørende behandlingssikkerked, tekniske og organisatoriske foranstaltninger, ansvar mellem dataansvarlige (vores kunder) og databehandler (HeroBase), og hvordan løsningen Hero Outbound gennem funktioner til bl.a. understøttelse af datasubjekternes rettigheder, understøtter vores kunder (de dataansvarlige) i at leve op til GDPR, for så vidt angår deres aktiviteter i Hero Outbound. Det beskrevne er altså gældende for vores leverance af produktet og ydelsen Hero Outbound til vores kunder.

UNDERSTØTTELSE AF FLERE KRAV



Systemejer er ansvarlig for, at sikre, at data kan slettes

- REGLER KAN GENBRUGES TIL AT UNDERSTØTTE FLERE LOVKRAV / STANDARDER OL.
- DET BLIVER **NEMMERE** AT TILFØJE NYE STANDARDER / LOVKRAV
  - F.eks. Er mange af vores kunder databehandlere, og vil gerne sikre understøttelse af ISAE3000 erklæringer

GENBRUG AF REGLER

1. 1. 3. RET TIL SLETNING ("RETTEN TIL AT BLIVE GLEMT") (ARTIKEL 17 OG ARTIKEL 19)

Der foreligger skriftlige procedurer, hvori håndtering af de registreredes ret til sletning af personoplysninger er beskrevet, eller hvordan databehandler kan bistå den dataansvarlige hermed.
Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.

FSR – ISAE 3000 Vejl.

Indirekte:

7. 1. 1. Fortegnelse over informationsaktiver

It-chefen har ansvar for, at alle it-aktiver bliver identificeret.

7. 1. 2. Fortegnelse over informationsaktiver

It-sikkerhedskoordinatoren sikrer at, der føres en fortegnelse over alle væsentlige it-aktiver, og at denne fortegnelse ajourføres løbende.

7. 1. 5. System til procesoverblik

Chefen for arkitekturafdelingen er ansvarlig for, at der til enhver tid, er etableret et system til at understøtte procesoverblikket for virksomhed X, hvori det er muligt at illustrere virksomhedens processer med tilhørende dataflows.

7. 1. 6. Opdatering af procesoverblik

Procesejer er ansvarlig for løbende at opdatere deres respektive procesoverblik med beskrivelser af, hvilke data der bliver anvendt i deres respektive processer, og hvor disse flyder hen

7. 1. 7. Kontrol af procesoverblik

Procesejer er ansvarlig for kvartalsvist at gennemløbe deres procesbeskrivelser samt flow og vurdere:

- Er der sket ændringer i mine behandling af data?
- Modtager/afgiver jeg andre data end de registrerede?
- Er der sket ændringer i hvor længe data er tilgængelige?

Egne regler

Skærmbillede fra ControlManager™

UDFORDRINGEN

Artikel 32

Behandlingssikkerhed

1. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

a) pseudonymisering og kryptering af personoplysninger

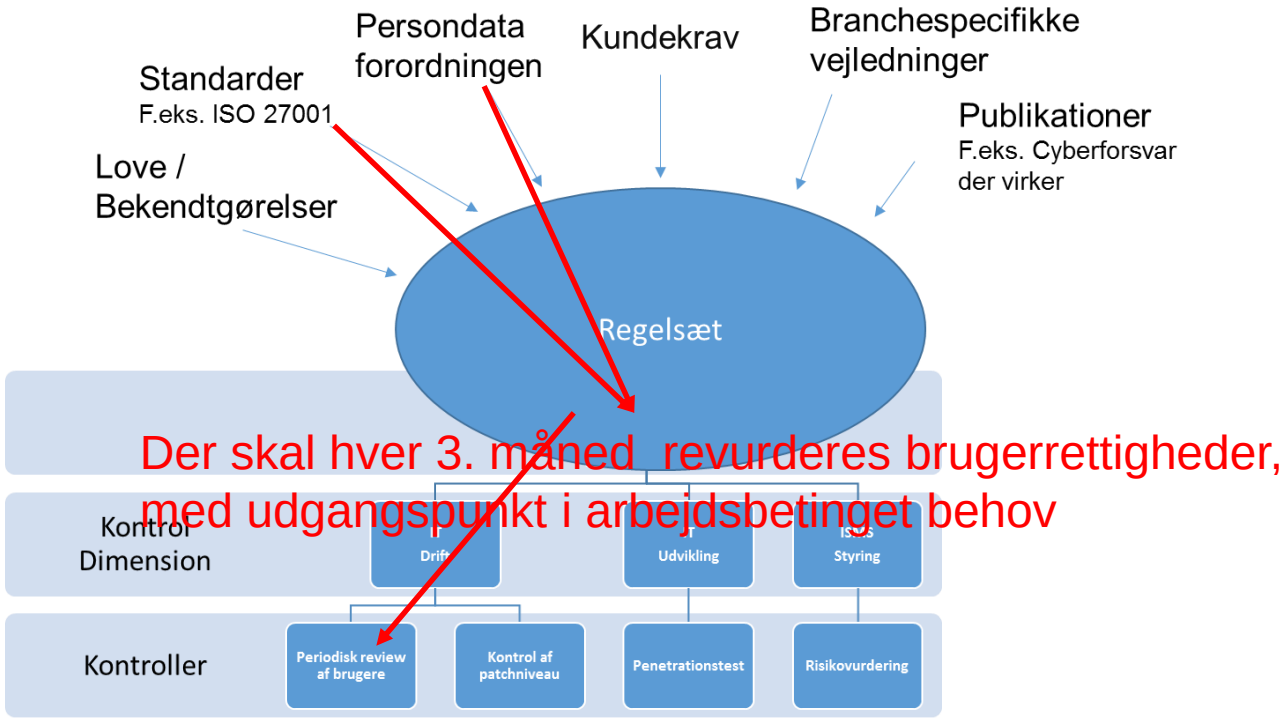
b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

- MED ANDRE ORD:
  1. Tekniske og organisatoriske foranstaltninger skal designes
     - En del af håndbogen
  2. Det skal sikres, at foranstaltningerne er effektive

FRA KRAV TIL ET SAMLET REGELSÆT



Der skal hver 3. måned revurderes brugerrettigheder, med udgangspunkt i arbejdsbetinget behov

- SAMMENHÆNG MELLEM:
  - LOV/STANDARD
  - REGLER
- UDBYGGES MED:
  - **KONTROLLER** - FOR AT SIKRE OVERHOLDELSE AF REGEL
  - **EVIDENS** SOM DOKUMENTATION FOR GENNEMFØRELSE

MAPNING AF EU-GDPR -> REGEL -> KONTROL - TILBAGE TIL EKSEMPLET

EU-GDPR

DATASUBJEKTET HAR RET TIL AT FÅ SLETTET PERSONDATA OM SIG SELV UDEN UNØDIG FORSINKELSE, OG DEN DATAANSVARLIGE HAR PLIGT TIL AT **SLETTE PERSONOPLYSNINGER** UDEN UNØDIG FORSINKELSE, HVIS DATA **ER IKKE LÆNGERE NØDVENDIGE** I FORHOLD TIL FORMÅLET ELLER,

Regel

Regel

Regel

PROCESEJER ER ANSVARLIG FOR LØBENDE AT OPDATERE PROCESOVERBLIKKET MED BESKRIVELSER AF HVILKE DATA DER BLIVER BEHANDLET I DERES RESPEKTIVE PROCESSER, OG HVOR DISSE FLYDER HEN

Hvordan/detaljer

Kontrol

HVER KVARTAL SKAL HVER PROCESEJER GENNEMLØBE DERES PROCESBESKRIVELSE SAMT FLOW OG VURDERE:

- Er der sket ændringer i min behandling af data?
- Modtager/afgiver jeg andre data en de registrerede?
- Er der sket ændringer i hvor længe data er nødvendige?

Hvordan

FRA PAPIRCOMPLIANCE -> FAKTUEL COMPLIANCE

Hero

SISCON
... styrker din position

3. 6. Artikel 17 – Ret til sletning (»retten til at blive glemt«)

3. 6. 1. stk. 1 (a), (b), (c), (d), (e), (f) ✔

Den dataansvarlige skal på datasubjektet anmodning og uden unødig forsinkelse slette persondata om datasubjektet, hvis:
- data ikke længere er nødvendige i forhold til formålet
- datasubjektet trækker sit samtykke tilbage
- gør indsigelse eller modsætter sig databehandlingen
- databehandlingen er ulovlig
- data skal slettes som følge af lovgivning
- angår indhentning af persondata om børn til brug i informationstjenester

”Krav jeg er underlagt”

Indirekte:

7. 1. 1. Fortegnelse over informationsaktiver

It-chefen har ansvar for, at alle it-aktiver bliver identificeret.

7. 1. 2. Fortegnelse over informationsaktiver

It-sikkerhedskoordinatoren sikrer at, der føres en fortegnelse over alle væsentlige it-aktiver, og at denne fortegnelse ajourføres løbende.

7. 1. 5. System til procesoverblik

Chefen for arkitekturafdelingen er ansvarlig for, at der til enhver tid, er etableret et system til at understøtte procesoverblikket for virksomhed X, hvori det er muligt at illustrere virksomhedens processer med tilhørende dataflows.

7. 1. 6. Opdatering af procesoverblik

Procesejer er ansvarlig for løbende at opdatere deres respektive procesoverblik med beskrivelser af, hvilke data der bliver anvendt i deres respektive processer, og hvor disse flyder hen

7. 1. 7. Kontrol af procesoverblik

Procesejer er ansvarlig for kvartalsvist at gennemløbe deres procesbeskrivelser samt flow og vurdere:

- Er der sket ændringer i mine behandling af data?
- Modtager/afgiver jeg andre data end de registrerede?
- Er der sket ændringer i hvor længe data er tilgængelige?

Egne regler – ”Hvad betyder det for mig?”

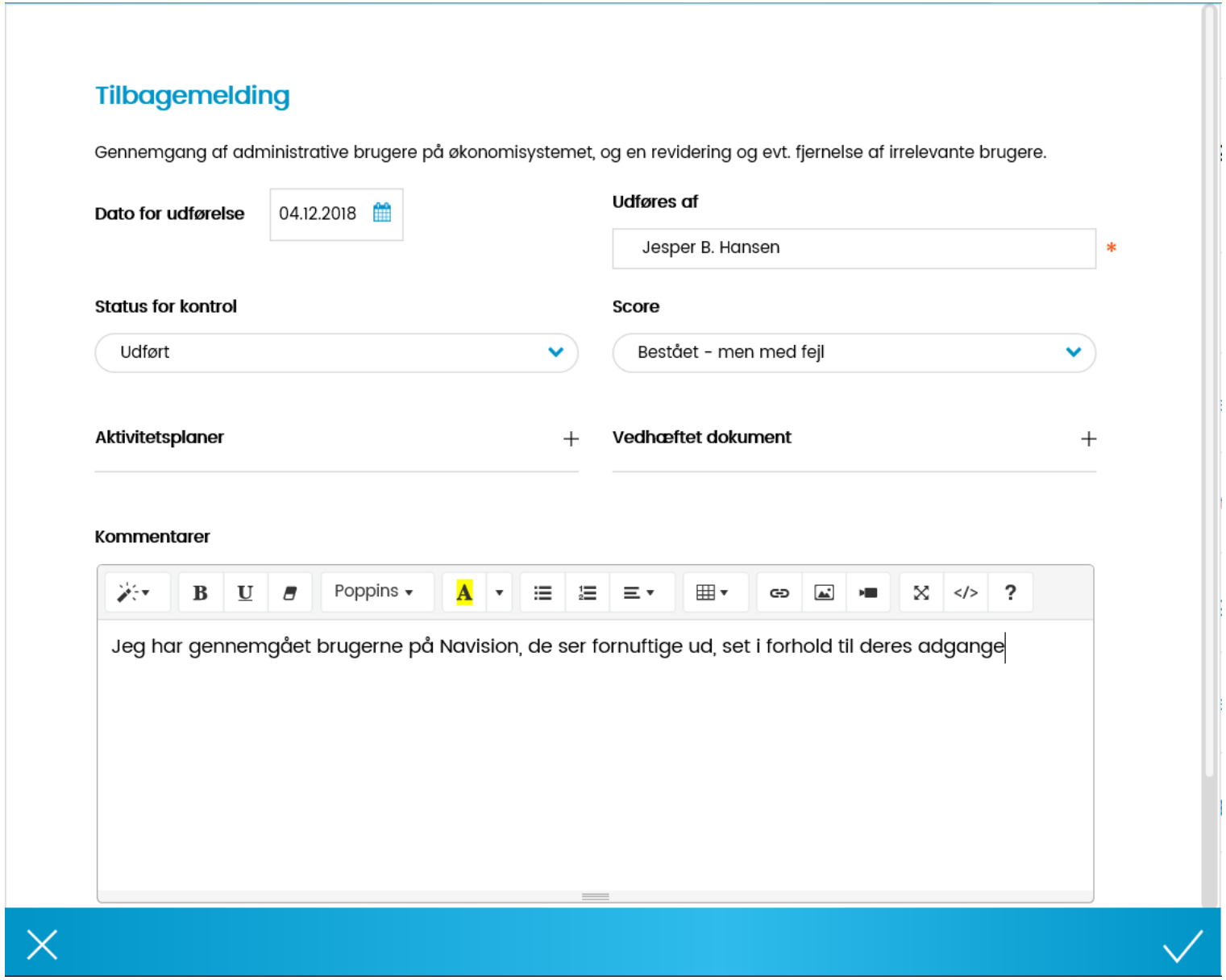
Kontroller til regler:

Kontrol af procesoverblik

Egen kontrol – ”Overholder jeg krav?”

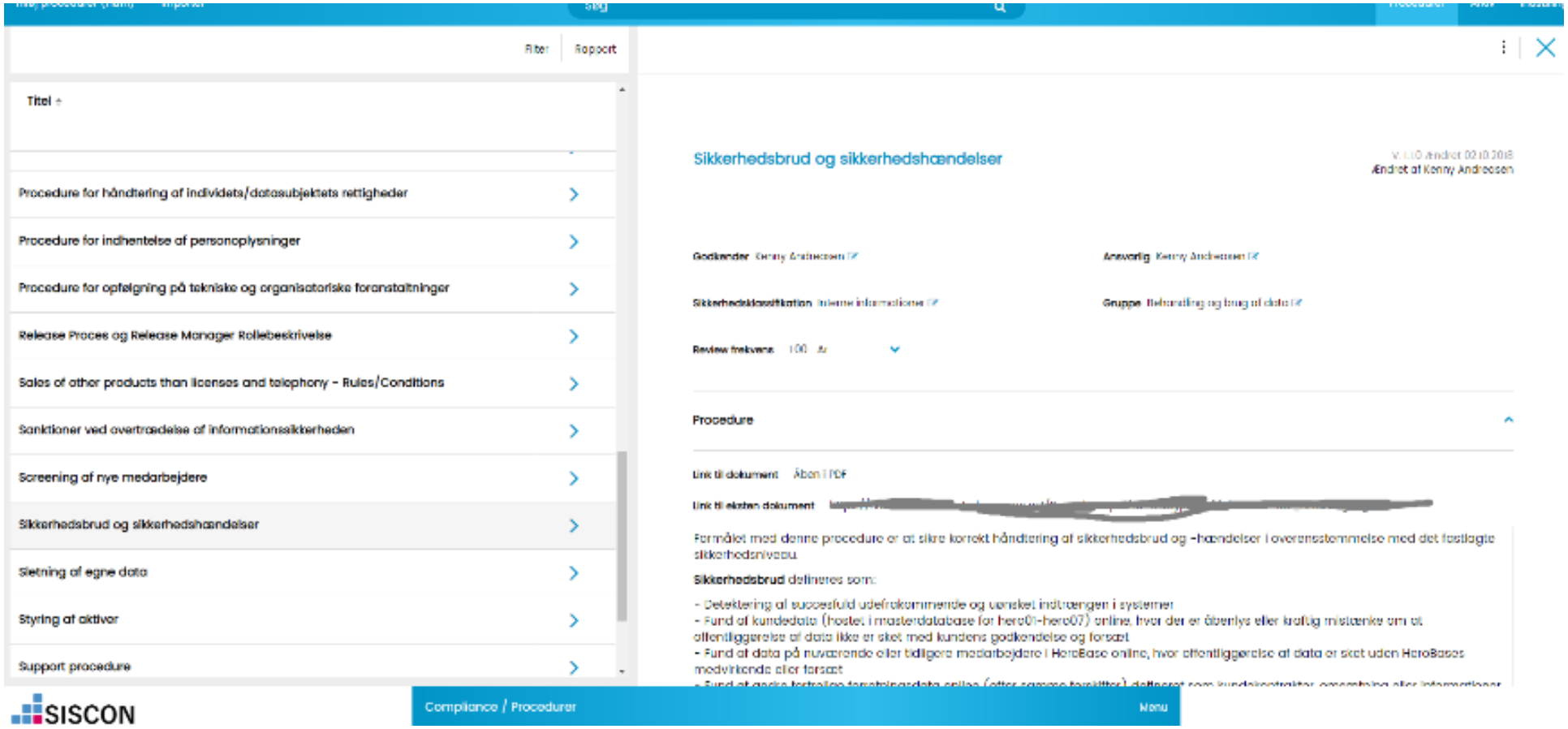
Skærmbillede fra ControlManager™

TILBAGEMELDING PÅ EN KONTROL



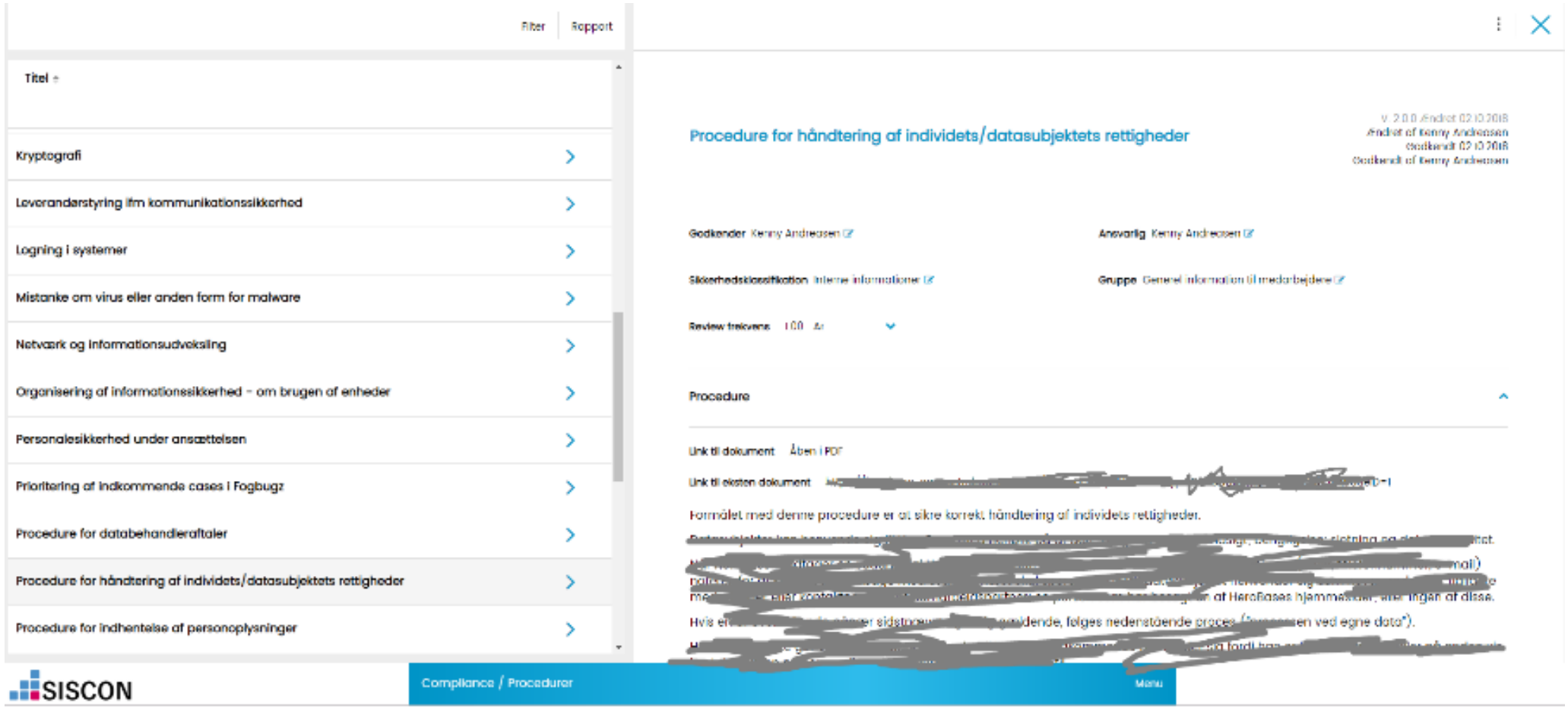
Hvorfor er det smart?

PROCEDURER SOM ”FAVNER DET HELE” (1)



Skærmbillede fra ControlManager™

PROCEDURER SOM ”FAVNER DET HELE” (2)



Skærmbillede fra ControlManager™

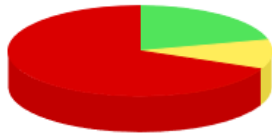
OVERSIGT OVER GENNEMFØRELSE AF KONTROLLER

Visning › | Logbog ›

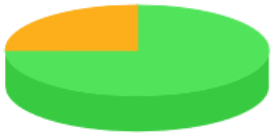
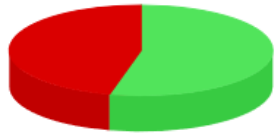
Gennemgang af brugere på Navision — **Logbog** 01.01.2014 - 06.09.2

Version 1.0 + Tilføj ekstra kontro

- 02.07.2018 - 07.07.2018 + Tilføj tilbagemelding
- 01.01.2018 - 06.01.2018 Seneste score: Bestået - men med fejl + Tilføj tilbagemelding
- 03.07.2017 - 08.07.2017 Seneste score: Bestået uden fejl + Tilføj tilbagemelding
- 02.01.2017 - 07.01.2017 Seneste score: Bestået uden fejl + Tilføj tilbagemelding
- 01.07.2016 - 06.07.2016 Seneste score: Bestået uden fejl + Tilføj tilbagemelding
- 01.01.2016 - 06.01.2016 + Tilføj tilbagemelding
- 01.07.2015 - 06.07.2015 + Tilføj tilbagemelding
- 01.01.2015 - 06.01.2015 + Tilføj tilbagemelding



Oversigt baseret på status med angivelse af %-vis udførelse

Udført / Delvis udført, perioden ikke udløbet	Ikke udført, perioden ikke udløbet / Ikke sta...	Delvist udført / Ikke udført / Ikke startet
		

Oversigt baseret på score af de enkelte kontroller

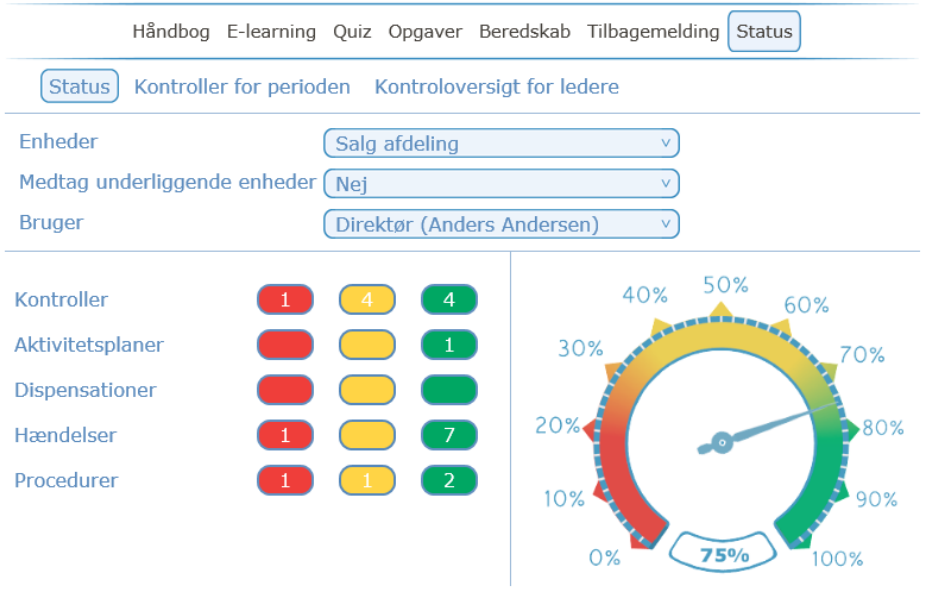
Udført / Delvis udført, perioden ikke udløbet	Ikke udført, perioden ikke udløbet / Ikke sta...	Delvist udført / Ikke udført / Ikke startet
		

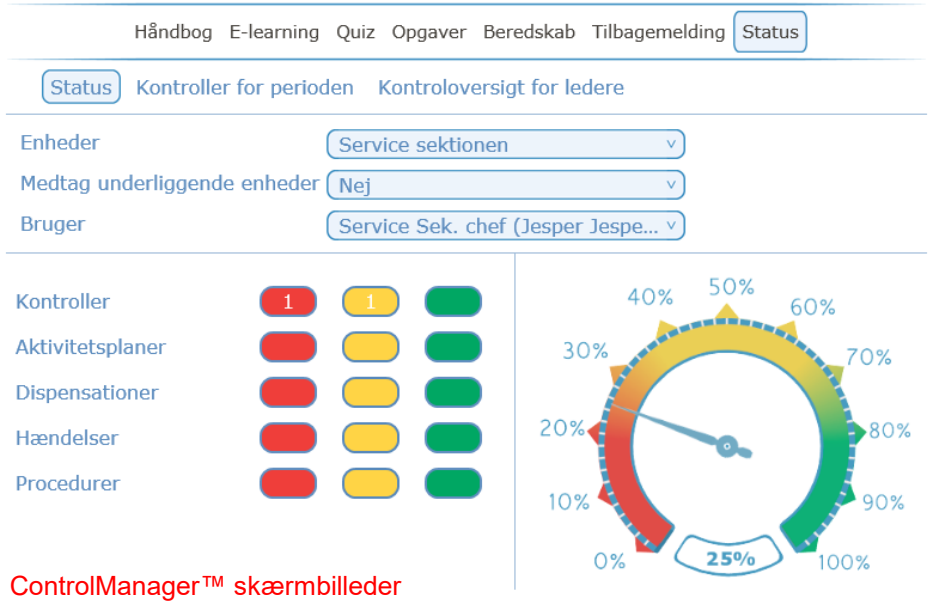
FORANKRING I FORRETNINGEN

- EN FOKUSERING PÅ KONTROLLER GIVER YDERMERE
  - Mulighed for at forankre og følge op på arbejdet ude i organisationen

- HVIS EU-GDPR SKAL FUNGERE SKAL DET VÆRE FORANKRET I FORRETNINGEN
  - De skal **tage ansvar**
  - De skal kende deres **eget** complianceniveau

- VI SKAL OPNÅ – **DOKUMENTERET VISHED**

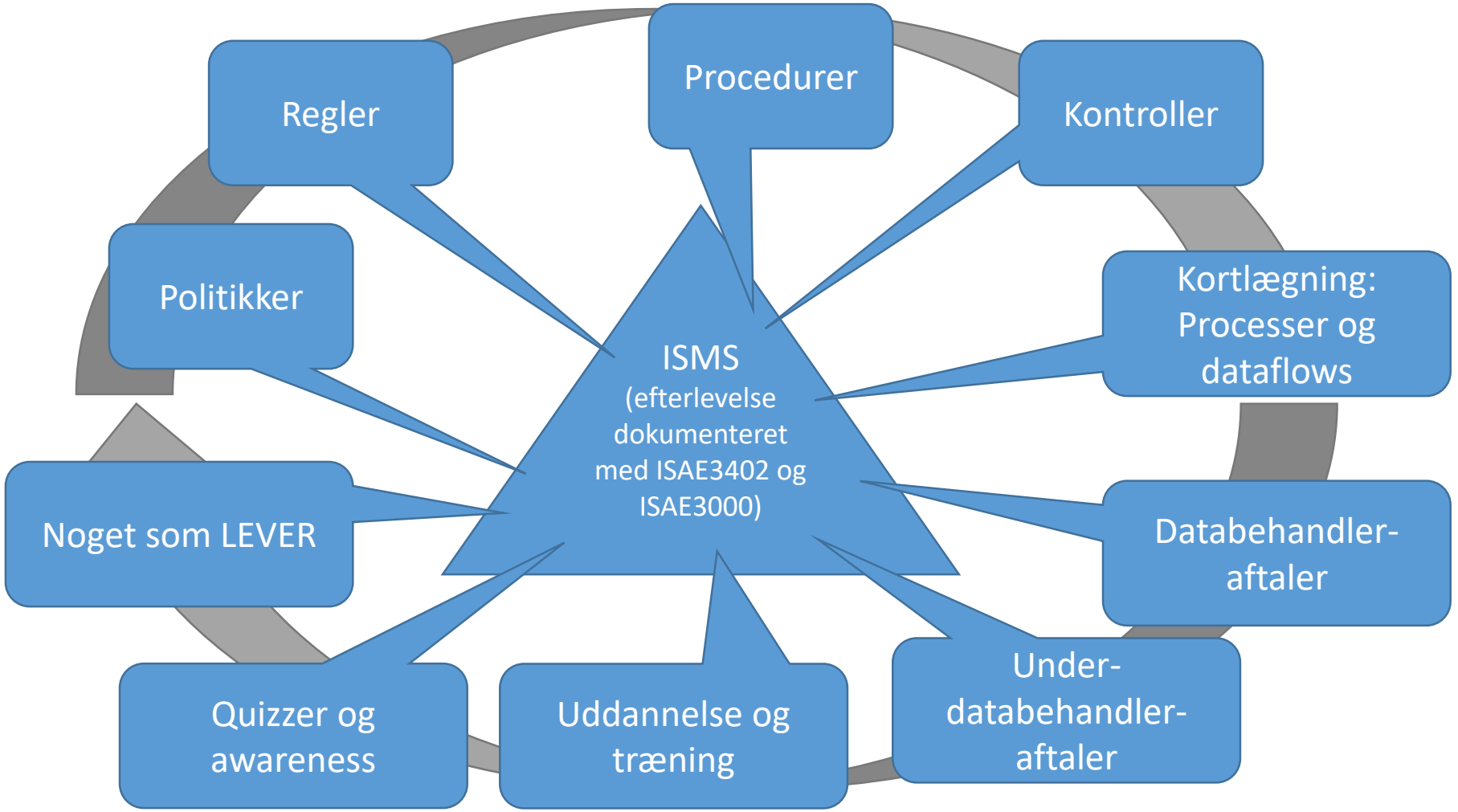




ControlManager™ skærmbilleder

FRA HIGH-LEVEL TIL LAVPRAKTISK

FORANKRING I FORRETNINGEN – DEN STORE SAMMENHÆNG

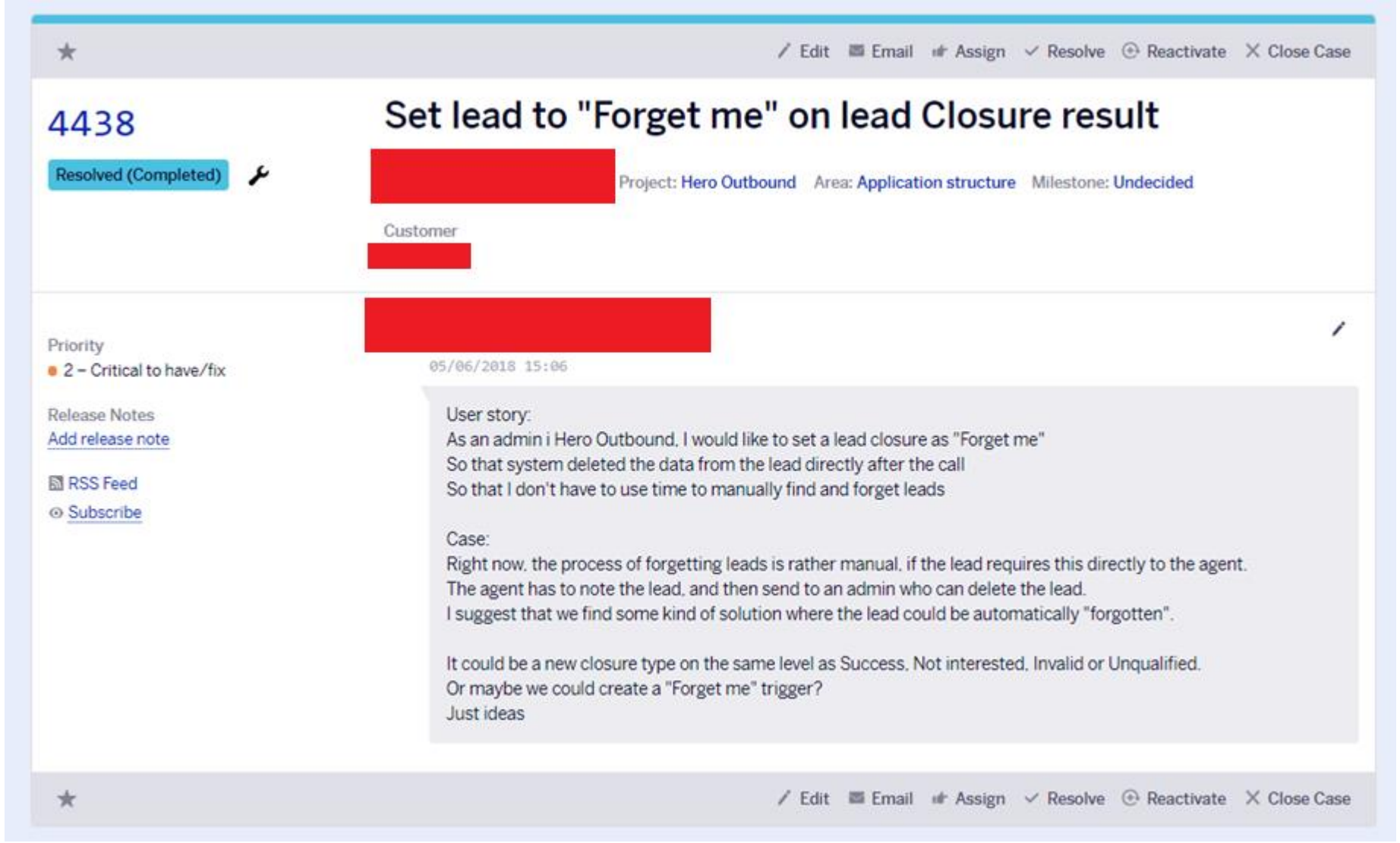


Gevinster

GEVINSTER

GEVINSTER

GEVINSTER


Edit
Email
Assign
Resolve
Reactivate
Close Case
4438
Set lead to "Forget me" on lead Closure result
Resolved (Completed)
[redacted]
Project: Hero Outbound
Area: Application structure
Milestone: Undecided
Customer
[redacted]
[redacted]
Priority
2 – Critical to have/fix
05/06/2018 15:06
Release Notes
Add release note
RSS Feed
Subscribe
User story:
As an admin i Hero Outbound, I would like to set a lead closure as "Forget me"
So that system deleted the data from the lead directly after the call
So that I don't have to use time to manually find and forget leads
Case:
Right now, the process of forgetting leads is rather manual, if the lead requires this directly to the agent.
The agent has to note the lead, and then send to an admin who can delete the lead.
I suggest that we find some kind of solution where the lead could be automatically "forgotten".
It could be a new closure type on the same level as Success, Not interested, Invalid or Unqualified.
Or maybe we could create a "Forget me" trigger?
Just ideas
Edit
Email
Assign
Resolve
Reactivate
Close Case

GEVINSTER

Uafhængig revisors erklæring med sikkerhed om
beskrivelsen af kontroller og deres udformning
i forbindelse med udvikling og drift af softwaren Hero Outbound
pr. 1. september 2018

ISAE 3402, type I

HeroBase A/S
CVR-nr. 31 07 31 03

September 2018

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. Kriterierne, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i HeroBase A/S' beskrivelse i afsnit 2, og det er på den baggrund vores vurdering,

(a) at beskrivelsen, således som det var udformet og implementeret per 1. september 2018, i alle væsentlige henseender er retvisende

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformede per 1. september 2018.

GEVINSTER

Hero

SISCON
... styrker din position

3: Den registreredes rettigheder

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
15 - Den registreredes indsigtsret	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til indsigt i egne registrerede personoplysninger og behandlingen heraf er overholdt.	Vi har forespurgt til procedure for håndtering af indsigtsanmodninger fra den registrerede, herunder underretning af databehandlere og modtagere af personoplysningerne, og vi har inspiceret proceduren. Vi har forespurgt til kontrol til sikring af overholdelse af virksomhedens procedure, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
16 - Ret til berigtigelse	Der efterleves procedurer og kontroller, som sikrer, at den registre-	Vi har forespurgt til procedure for berigtigelse af personoplysninger, herunder underretning af databe-	Ingen væsentlige afvigelser konstateret.
pligt i forbindelse med berigtigelse eller sletning af personop-	egne registrerede personoplysninger er overholdt, herunder sletning hos modtagere af	at databehandlere bliver underrettet om at slette persondata, og vi har inspiceret proceduren.	

Erklæring fra uafhængig revisor

Erklæringsafgivelse i forbindelse med overholdelse af databeskyttelsesforordningen (GDPR) pr. 17. december 2018

ISAE 3000

HeroBase A/S

CVR-nr.: 31 07 31 03

December 2018

Konklusion

Denne konklusion er udformet på grundlag af forståelsen af de kriterier, som der er redegjort for i erklæringens indledende afsnit, og som bygger på kravene i databeskyttelsesforordningen (GDPR).

Det er vores opfattelse, at HeroBase A/S' løsning Hero Outbound, i alle væsentlige henseender, lever op til ovennævnte kriterier pr. dags dato, 17-12-2018.

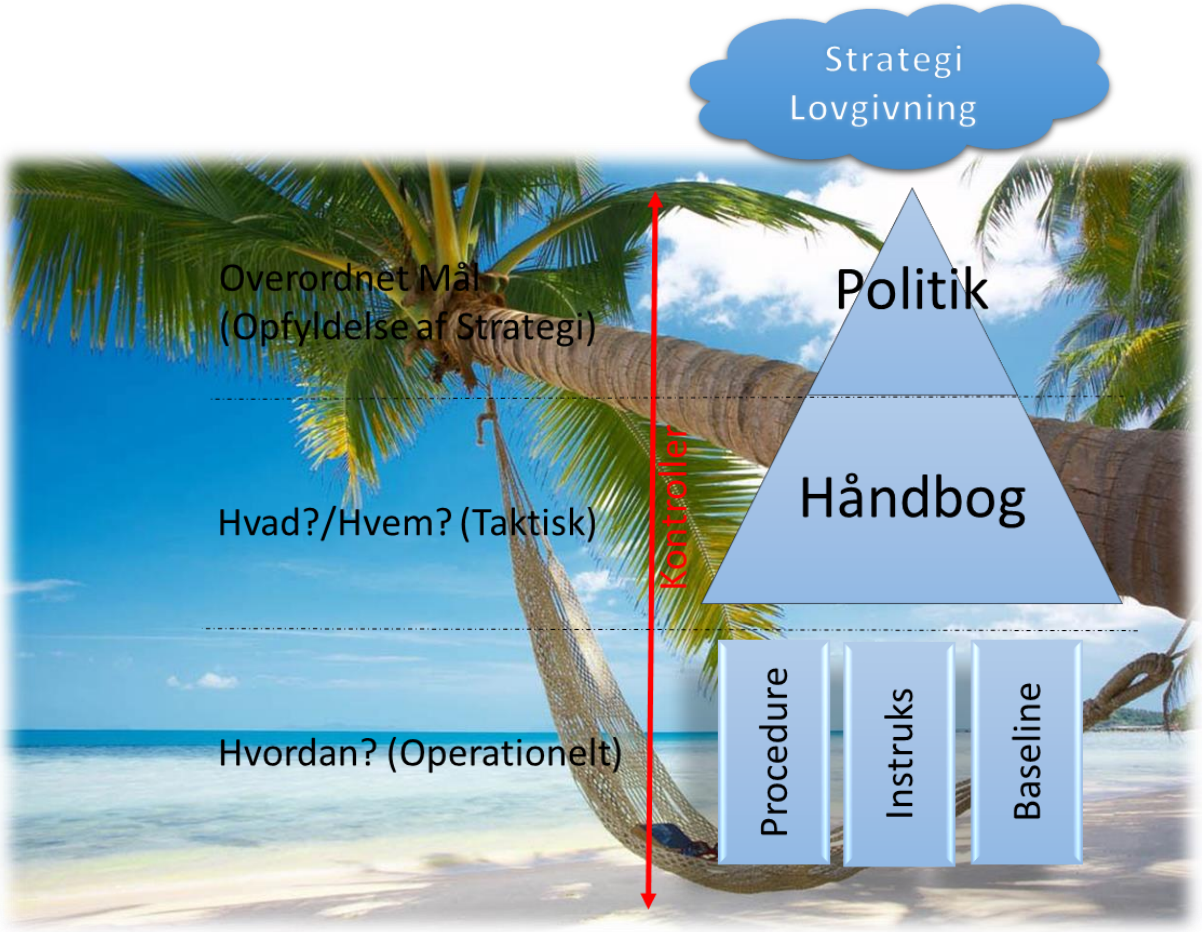
YOUR TAKE-AWAY

GEVINSTEN

- HUSK – DU SKAL IKKE GØRE DET ALENE FOR TILSYN / REVISIONENS SKYLD
  - Du skal gøre det, fordi det **skaber værd**i i praksis
  - Det kan være med til at højne sikkerheden generelt

- VED AT IMPLEMENTERE DET FORESLÅEDE, FÅR DU:
  - tolket forskellige rammer i forhold til, hvad de betyder for dig og din organisation
  - defineret **roller og ansvar** i din organisation
  - skabt **løbende overblik** over dit compliance**n**iveau
  - etableret muligheden for løbende at opdage og imødekomme problemer - også **før** tilsynet kommer

- DU FÅR SELV **RO I MAVEN** OG KAN **MÅSKE SLAPPE LIDT AF I HÆNGEKØJEN**☺



TAK FORDI I LYTTEDE !

Kontaktinformationer:

Jesper B. Hansen
Senior Implementeringskonsulent
Siscon ApS
E-mail: jbh@siscon.dk

Kenny Andreasen
CTO & CIO
HeroBase A/S
E-mail: ka@herobase.com

SISCON
... styrker din position

Hero