

# Region Hovedstadens informationssikkerheds- politik

# Indholdsfortegnelse

<b>1. Indledning</b> .....	<b>3</b>
Hvad er informationssikkerhed? .....	3
<b>2. Formål med informationssikkerheds-politikken</b> .....	<b>4</b>
Ydre rammer for arbejdet med informations- .....	4
sikkerhed.....	4
<b>3. Gyldighedsområde</b> .....	<b>5</b>
<b>4. Målsætninger</b> .....	<b>5</b>
<b>5. Informationssikkerhedsledelse</b> .....	<b>6</b>
Principper for informationssikkerhedsledelse .....	6
Organisering af informationssikkerhedsledelse .....	7
<b>6. Persondat beskyttelse</b> .....	<b>7</b>
Hvad er en personoplysning? .....	7
Principper for behandling af personoplysninger .....	8
Databeskyttelsesrådgiver (DPO) .....	8
Databehandlere og lovlig videregivelse .....	9
Overførsel til tredjelande.....	9
Fortegnelse .....	9
Registreredes rettigheder .....	10
Klagemuligheder.....	10
<b>7. Risikostyring</b> .....	<b>10</b>
Konsekvensanalyse.....	11
Risikovurdering af konkrete systemer og teknologi .....	11
<b>8. Sikkerhedshændelser</b> .....	<b>12</b>
<b>9. Beredskab</b> .....	<b>12</b>
<b>10. Sikkerhedskultur</b> .....	<b>12</b>

<b>11. Dispensation .....</b>	<b>13</b>
<b>12. Sanktioner.....</b>	<b>13</b>
<b>13. Godkendelse og revision .....</b>	<b>13</b>

Version: 5  
Udformet af: Sektion for Informationssikkerhed  
Senest opdateret: 7. februar, 2025

# 1. Indledning

Region Hovedstaden bruger dagligt data som led i regionens opgaveløsning inden for sundhed, forskning, regional udvikling og det sociale område. Især på sundhedsområdet har regionen ansvar for mange følsomme data om borgernes helbred. I Region Hovedstaden har vi både borgernes liv og data i vores hænder. Informationssikkerhed er derfor højt prioriteret i regionen.

Adgangen til data er central for det daglige arbejde, og som offentlig myndighed har regionen ansvar for at passe godt på de data, som borgere, virksomheder og andre samarbejdspartnere har betroet os. Samtidig skærper trusselsbilledet med stigende cyberkriminalitet samt kompleks databeskyttelseslovgivning kravene til regionens sikkerhed.

Arbejdet med informationssikkerhed understøtter Region Hovedstadens vision, mission, værdier og strategiske målsætninger. Et stærkt fokus på informationssikkerhed bidrager aktivt til regionens vision om at være en innovativ metropol med høj vækst og livskvalitet, samt et sammenhængende sundhedsvæsen på internationalt topniveau ved at:

- Fremme livskvalitet og patienttilfredshed, fordi borgerne er trygge og har tillid til, at regionen passer godt på deres personoplysninger
- Styrke regionens omdømme og sætte professionelle rammer og standarder for informationssikkerhed, der gør regionen til en attraktiv samarbejdspartner inden for forskning, udvikling og innovation
- Understøtte regionens kerneforretning og sikre adgangen til data, som en del af grundlaget for at kunne drive og udvikle et effektivt sundhedsvæsen med sammenhængende patientforløb.

I det daglige arbejde skal informationssikkerhed derfor være en integreret del af regionens drifts- og udviklingsopgaver og medvirke til, at borgere, samarbejdspartnere og andre interessenters tillid til regionen fastholdes. Høj databeskyttelse er ydermere en forudsætning for forskning på topplan og bedre anvendelse af sundhedsdata til gavn for patienter og borgere.

## Hvad er informationssikkerhed?

Grundelementet i informationssikkerhed er at beskytte informationer, så deres *fortrolighed*, *integritet* og *tilgængelighed* bevares. I praksis betyder det, at regionen skal sikre, at uvedkommende ikke har adgang til informationer (fortrolighed), at informationer ikke er manipulerede eller uretmæssigt ændret (integritet), og at autoriserede personer kan få adgang til informationer, når det er nødvendigt (tilgængelighed). Informationer kan i denne sammenhæng både være fysiske og digitale. I Region Hovedstaden omfatter arbejdet med informationssikkerhed både it-sikkerhed, persondatabeskyttelse samt organisering og ledelse.

## 2. Formål med informationssikkerheds- politikken

Formålet med Region Hovedstadens informationssikkerhedspolitik er at fastlægge de overordnede rammer, organisering og ansvar, principper og målsætninger for arbejdet med informationssikkerhed i Region Hovedstaden.

Region Hovedstadens informationssikkerhedspolitik tager udgangspunkt i og udmønter "Fællesregional informationssikkerhedspolitik", som er udarbejdet i et samarbejde mellem Region Hovedstaden, Region Sjælland, Region Syddanmark, Region Midtjylland og Region Nordjylland og godkendt af regionsrådet i Region Hovedstaden i januar 2017. Samtidig understøtter informationssikkerheds-politikken den fællesregionale (eksterne) persondatapolitik, som inden for rammerne af den overordnede fællesregionale informationssikkerhedspolitik, sætter fokus på persondatabeskyttelse og kommunikation til borgere og andre eksterne interessenter.



Figur 1: Regelhierarki for informationssikkerhed og databeskyttelse i Region Hovedstaden

Informationssikkerhedspolitikken udmøntes gennem retningslinjer, vejledninger, instrukser m.m., der sikrer, at alle medarbejdere arbejder med og forholder sig til informationssikkerhed og databeskyttelse, som led i det daglige arbejde i Region Hovedstaden.

## Rammer for arbejdet med informations- sikkerhed

Arbejdet med informationssikkerhed i Region Hovedstaden tager afsæt i god praksis for it-sikkerhed og følger principperne i ISO27001 standarden, som er baseret på en risikobaseret tilgang til styring af informationssikkerhed.

Lovgrundlaget for arbejdet med informationssikkerhed og denne politik er Databeskyttelseslovgivningen, som består af EU's Forordning om databeskyttelse (GDPR) og Databeskyttelsesloven. Databeskyttelsesloven fastsætter nationale regler, som supplerer de ge-

nerelle bestemmelser i EU's Forordning om databeskyttelse. Adgangen til og behandlingen af data og personoplysninger i regionen kan dog være reguleret i flere andre love, som politikken ikke berører for eksempel Sundhedsloven, Forvaltningsloven, Offentlighedsloven, Autorisationsloven, Serviceloven, Lægemiddeloven og Apotekerloven. Herudover indeholder lovgivning relateret til NIS-direktivet sektorspecifikke krav til sikkerheden i net- og informationssystemer, eksempelvis på sundhedsområdet.

Endelig refererer arbejdet med informationssikkerhed i Region Hovedstaden til nationale strategier og aftaler på digitaliserings- og sikkerhedsområdet for eksempel "Digitalisering der løfter samfundet", "Den fællesoffentlige digitaliseringsstrategi 2022-2025", "Ét sikkert og sammenhængende sundhedsnetværk for alle", "Strategi for digital sundhed 2018-2024", og "National strategi for cyber- og informationssikkerhed 2022-2024".

Derudover sætter Region Hovedstadens samlede strategi for cyber- og informationssikkerhed 2024-2027 retningen for udvikling af regionens modenhed og samler trådene fra ny lovgivning og initiativer på området.

### 3. Gyldighedsområde

Informationssikkerhedspolitikken gælder for alle brugere i Region Hovedstaden, herunder medarbejdere, forskere, konsulenter, regionsrådsmedlemmer, elever, studerende og andre, der midlertidigt eller for en længere periode har adgang til data og personoplysninger, som regionen er ansvarlig for.

Relevante krav til eksterne samarbejdspartnere og leverandører vedrørende informationssikkerhed skal indarbejdes og konkretiseres i aftaleforholdet, således at regionens sikkerhedsniveau fastholdes og sikres. Når flere regioner anvender samme samarbejdspartner eller leverandør til fælles løsninger, skal den fællesregionale informationssikkerhedspolitik anvendes.

### 4. Målsætninger

Region Hovedstaden har følgende overordnede målsætninger for informationssikkerhed:

- Regionens sikkerhedsniveau skal fastlægges ud fra en risikobaseret tilgang, som balancerer sikkerhedshensyn og efterlevelse af databeskyttelseslovgivningen med forretningshensyn
- Borgere, patienter, virksomheder, samarbejdspartnere og andre interessenter skal have tillid til, at regionen har etableret de nødvendige tiltag til at beskytte data, og at regionen forvalter deres personoplysninger sikkert og forsvarligt

- Regionen skal arbejde professionelt og struktureret med informationssikkerhed ved at følge ISO27001 standarden som ramme for informationssikkerhedsledelse og -styring
- Alle medarbejdere i regionen skal være bevidste om, at de spiller en vigtig og aktiv rolle i forhold til regionens samlede informationssikkerhed. De skal kende og efterleve regler og retningslinjer for informationssikkerhed, som er relevante i deres daglige arbejde og være engageret i regionens uddannelses- og træningsaktiviteter på området.

Regionen skal gennem leverandørstyring og kontrakter, for eksempel databehandleraftaler, stille krav til eksterne samarbejdspartnere og leverandører vedrørende informationssikkerhed og følge op på dem.

## 5. Informationssikkerhedsledelse

Ledelsen af informationssikkerhedsarbejdet i Region Hovedstaden sker efter en række overordnede principper, og er organiseret på to forskellige niveauer: et rammesættende og et udmøntende niveau, hvor regionens forskellige aktører i informationssikkerhedsarbejdet har hver deres rolle, opgaver og ansvar.

### Principper for informationssikkerhedsledelse

Ledelsen af informationssikkerhedsarbejdet i Region Hovedstaden er baseret på følgende principper:

- Informationssikkerhed skal være forankret i regionens politiske og administrative topledelse
- Informationssikkerhed skal indarbejdes i den eksisterende organisation og ledelsesstruktur
- Ansvar for efterlevelse af regionens informationssikkerhedspolitik, retningslinjer, vejledning m.m. og ansvar for overholdelse af databeskyttelseslovgivningen skal ligge i de organisatoriske enheder/linjeorganisationen.

Inden for de rammer, der er fastlagt i regionens informationssikkerhedspolitik og retningslinjer, skal beslutninger vedrørende informationssikkerhed og databeskyttelse så vidt muligt tages tæt på de berørte forretningsområder.

## Organisering af informationssikkerhedsledelse

Det rammesættende niveau af informationssikkerhedsledelse i Region Hovedstaden udgøres af regionens politiske og administrative topledelse. Regionsrådet har det øverste ansvar for at fastlægge den overordnede ramme og retning for arbejdet med informationssikkerhed i Region Hovedstaden, herunder at godkende Region Hovedstadens informationssikkerhedspolitik. Koncernledelsen har ansvar for den administrative styring af arbejdet med informationssikkerhed i regionen. Digital Styregruppe (DS) varetager i praksis koncernledelsens opgaver på området.

Det udmøntende niveau udgøres af direktioner, linjeledelser og medarbejdere i regionens hospitaler, virksomheder og centre, som alle har bestemte opgaver og ansvar i forhold til at udmønte og efterleve informationssikkerhedspolitikken i praksis.

Hospitals-, virksomheds- og centerdirektionerne har det overordnede ansvar for at implementere og efterleve informationssikkerhedspolitikken og retningslinjer for informationssikkerhed og databeskyttelse i egen organisatorisk enhed. Direktioner i regionens koncerncentre har derudover en særlig opgave i forhold til at udmønte retningslinjer, som er målrettet de regionale rammer og services, som centret har et tværgående ansvar for. Linjeledelser og medarbejdere har ansvar for at efterleve de regler og retningslinjer i den daglige opgaveløsning, som knytter sig til deres rolle og arbejdsopgaver.

Til at understøtte både det rammesættende og udmøntende niveau har regionen etableret en central informationssikkerhedsfunktion – Sektion for Informationssikkerhed, som styrer, tilrettelægger og driver arbejdet med informationssikkerhed. Sektion for Digital Compliance har det overordnede ansvar for, hvordan databeskyttelseslovgivningen fortolkes og udmøntes i regionen.

## 6. Persondatabeskyttelse

Åbenhed og professionalisme i omgangen med persondata medvirker til at fastholde borgernes tillid og regionens troværdighed. Behandling af personoplysninger i Region Hovedstaden skal derfor ske med omhu og overholde reglerne i databeskyttelseslovgivningen. Behandling er i denne sammenhæng de aktiviteter, som sker med personoplysninger. Det kan for eksempel være indsamling, registrering, bearbejdning, opbevaring, offentliggørelse, ændring, søgning, overførsel og sletning af personoplysninger.

### Hvad er en personoplysning?

Personoplysninger er enhver form for information, som alene eller sammen med andre oplysninger kan henføres til en bestemt fysisk person. Databeskyttelseslovgivningen skelner

mellem forskellige kategorier af personoplysninger, der har betydning for kravene til, hvordan personoplysninger skal behandles.

*Følsomme personoplysninger* er helbredsoplysninger, oplysninger om race eller etnisk oprindelse, oplysninger om politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, oplysninger om en persons seksuelle orientering eller seksuelle forhold samt genetisk og biometrisk data, der har til formål at identificere en bestemt person.

CPR-numre og oplysninger om strafbare forhold er to kategorier af personoplysninger, som har særstatus i lovgivningen. Det betyder, at de i praksis skal behandles på lige fod med følsomme oplysninger i Region Hovedstaden.

Alle andre personoplysninger falder ind under kategorien *almindelige personoplysninger*. Det er for eksempel navn, fødselsdato, alder, adresse, interesser, økonomiske og sociale forhold, CV, ansøgning m.m.

## Principper for behandling af personoplysninger

Personoplysninger, som regionen har ansvar for, skal behandles i overensstemmelse med følgende principper i Databeskyttelsesforordningen:

- Personoplysninger skal behandles lovligt, rimeligt og gennemsigtigt
- Personoplysninger skal indsamles til udtrykkeligt angivne og saglige formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål
- Personoplysninger skal være tilstrækkelige, relevante og begrænset til formålet
- Personoplysninger skal være korrekte og ajourførte
- Personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i længere tid end det er nødvendigt til formålet
- Personoplysninger skal behandles, så der er tilstrækkelig sikkerhed for personoplysningerne.

Behandling af personoplysninger i Region Hovedstaden er på nogle områder reguleret af anden lovgivning, for eksempel Sundhedsloven, som fastsætter særlige regler for bl.a. opbevaring af journaler og sletning af oplysninger i journalerne.

## Databeskyttelsesrådgiver (DPO)

Region Hovedstaden har en uafhængig databeskyttelsesrådgiver (DPO), som skal rådgive regionen og inddrages i principielle og væsentlige beslutninger vedrørende databeskyttelse samt føre tilsyn med, at regionen overholder databeskyttelseslovgivningen.

## Databehandlere og lovlig videregivelse

Region Hovedstaden samarbejder som offentlig myndighed med forskellige eksterne parter, bl.a. private virksomheder og andre offentlige myndigheder. Det kan eksempelvis være, når en virksomhed leverer et it-system eller en service til regionen, eller når en offentlig myndighed beder regionen om at videregive personoplysninger. Inden regionen overfører personoplysninger til en ekstern part, skal det fastslås, hvorvidt den eksterne part i den konkrete situation er databehandler for regionen eller bliver selvstændigt dataansvarlig som følge af en lovlig videregivelse.

En *dataansvarlig* bestemmer, til hvilke formål og hvordan personoplysningerne må behandles. Det er den dataansvarlige, der har ansvaret for, at behandlingen af personoplysninger lever op til reglerne i databeskyttelseslovgivningen. En *databehandler* behandler udelukkende personoplysninger på vegne af og efter instruks fra den dataansvarlige. *Videregivelse* betyder, at den dataansvarlige (den videregivende part) har et lovligt grundlag til at overføre personoplysninger til en ekstern part, som derefter bliver selvstændig dataansvarlig for viderebehandlingen af de modtagne personoplysninger.

Regionen skal som dataansvarlig indgå en skriftlig databehandleraftale, når en ekstern part behandler personoplysninger på vegne af regionen. Omvendt er der ved videregivelse af personoplysninger krav om et lovligt grundlag for overførslen.

Regionerne har udarbejdet en fællesregional databehandlerskabelon, som skal benyttes, når regionen er dataansvarlig, og der skal indgås en databehandleraftale.

Videregivelse er et særligt begreb i databeskyttelseslovgivningen, som handler om overførslen af personoplysninger fra en dataansvarlig til en anden dataansvarlig og skal ikke forveksles med videregivelsesbegrebet i Sundhedsloven.

## Overførsel til tredjelande

Der gælder særlige regler, når regionen overfører personoplysninger til tredjelande og internationale organisationer, der befinder sig i et tredjeland. Tredjelande er lande, som ikke er medlem af EU eller EØS (Island, Liechtenstein og Norge). En overførsel kan både bestå i en direkte transmission af data, og at personer i et tredjeland har "se-adgang" til personoplysninger, der befinder sig i EU. Hvis der skal overføres personoplysninger til tredjelande, skal EU Kommissionens Standardkontraktbestemmelser anvendes.

## Fortegnelse

Region Hovedstaden skal føre en fortegnelse over de behandlingsaktiviteter, som regionen er ansvarlig for. Fortegnelsen fungerer som dokumentation for, hvordan Region Hovedstaden behandler data og vil bl.a. blive benyttet af Datatilsynet i forbindelse med tilsyn.

Sektion for Digital Compliance ejer Fortegnelsen i Region Hovedstaden. Region Hovedstaden har herudover en særlig fortegnelse for forskningsprojekter, som ejes af Forskningsjura på Rigshospitalet.

## Registreredes rettigheder

Borgere, patienter og medarbejdere, hvis personoplysninger regionen behandler (også kaldet registrerede) har en række rettigheder i forhold til brugen af deres oplysninger. Registrerede i Region Hovedstaden har bl.a. ret til indsigt i regionens behandling af deres personoplysninger, ret til berigtigelse af urigtige personoplysninger om dem, ret til begrænsning af behandling af personoplysninger om dem (for eksempel hvis der er uklarheder om rigtigheden af oplysningerne) og ret til at gøre indsigelse mod behandlingen af deres oplysninger.

Når regionen får eller indsamler personoplysninger, har regionen pligt til at give de registrerede en række informationer om behandlingen af deres data, som følge af regionens oplysningspligt, bl.a. formålet og lovgrundlaget for behandlingen.

I nogle tilfælde vil de registreredes rettigheder være begrænset af anden lovgivning, for eksempel Databeskyttelsesloven eller Sundhedsloven.

Regionerne har udarbejdet en fællesregional (ekstern) persondatapolitik, som fortæller borgere, brugere og patienter, hvordan regionerne behandler og beskytter deres personoplysninger. Persondatapolitikken er tilgængelig på Region Hovedstadens hjemmeside.

## Klagemuligheder

Borgere, patienter og medarbejdere har mulighed for at klage til Datatilsynet, hvis de mener, at Region Hovedstaden ikke behandler deres personoplysninger korrekt i forhold til databeskyttelseslovgivningen. Inden opfordres de til at tage kontakt til regionen således, at sagen kan undersøges. Registrerede kan også kontakte regionens databeskyttelsesrådgiver.

## 7. Risikostyring

Region Hovedstadens tilgang til risikostyring følger principperne i ISO27001 og har til formål at sikre, at de rette i Region Hovedstadens ledelseslag (jf. afsnit 5. Informationssikkerhedsledelse) systematisk og løbende forholder sig til og træffer beslutning om risici vedrørende informationssikkerhed.

Præsenteret for en konkret risiko er det ledelsens opgave at vurdere sandsynlighed og konsekvens ved risikoen og lægge de overordnede rammer for risikohåndteringen ud fra en af følgende strategier:

- **Acceptér:** Risikoen accepteres, og der foretages ikke yderligere
- **Mitigér/kontroller:** Risikoen styres ved at indføre kontroller eller foranstaltninger, som fjerner eller reducerer sandsynligheden eller konsekvenserne
- **Undgå:** Risikoen undgås ved at stoppe eller ændre den aktivitet, som er årsag til risikoen
- **Overfør/Del:** Risikoen overføres til en tredjepart

Når informationssikkerhedsledelsen skal fastlægge en strategi for risikohåndteringen, skal følgende hensyn tilgodeses og balanceres:

- Regionens samlede informationssikkerhed
- Kvalitet i patientbehandling eller anden kerneforretning
- Økonomi og ressourcer
- Effektivitet i opgaveløsningen
- Hensynet til den registrerede og dennes rettigheder

Regionens retningslinjer for risikostyring er yderligere beskrevet i ”Supplerende retningslinje for informationssikkerhed og databeskyttelse: Risikostyring”.

## Konsekvensanalyse

Regionen skal som dataansvarlig udarbejde en konsekvensanalyse, når en behandling sandsynligvis vil indebære en høj risiko for, at den registrerede kan få krænket sine rettigheder og frihedsrettigheder. Formålet er at belyse og håndtere de personlige og sociale konsekvenser, for eksempel krænkelser af privatlivets fred og identitetstyveri, der kan være ved brug af nye digitale løsninger, teknologier og services. Konsekvensanalyser skal udarbejdes, inden databehandlingen igangsættes, og databeskyttelsesrådgiveren skal rådføres i processen.

## Risikovurdering af konkrete systemer og teknologi

Regionen skal, som led i forvaltningen af systemer og teknologier, løbende gennemføre risikovurderinger og sikre, at der fastlægges strategier for håndteringen af identificerede risici. Risikovurderingerne skal gennemføres med en kadence og en dybde, som står i forhold til systemerne og teknologiernes kritikalitet.

## 8. Sikkerhedshændelser

Alle sikkerhedshændelser og brud på persondatasikkerheden skal rapporteres til Center for IT og Medicoteknologi (CIMT) via CIMT Service eller ved at kontakte CIMT Service-desk. Sikkerhedshændelser er hændelser, hvor regionens it-systemer i en periode har været underkastet en lavere sikkerhed end normalt og/eller hændelser, der har medført et tab af integritet eller fortrolighed af kritiske forretningsdata (uden personoplysninger).

Der er tale om et brud på persondatasikkerheden, hvis personoplysningers fortrolighed, integritet eller tilgængelighed er blevet kompromitteret. Brud på persondatasikkerheden skal dokumenteres og i nogle tilfælde indberettes til Datatilsynet. Indberetningen til Datatilsynet skal foretages senest 72 timer efter, at det er konstateret, at der er sket et brud. De registrerede personer, som bruddet omfatter, skal informeres, hvis regionen vurderer, at bruddet medfører en høj risiko for deres rettigheder, for eksempel diskrimination, identitetstyveri eller svig, økonomisk tab, skade på omdømme eller sociale konsekvenser. Den centrale tovholderfunktion for brud på persondatasikkerheden, som pt. er Sektion for Informationssikkerhed, står for dokumentation og eventuel indberetning til Datatilsynet.

## 9. Beredskab

Alle organisatoriske enheder i Region Hovedstaden har deres egne lokale beredskabsplaner. Center for IT og Medicoteknologi (CIMT) har ansvaret for it-beredskabet for regionens infrastruktur og forretningskritiske systemer, og for at der er foreliggende en it-beredskabsplan. Det primære formål med it-beredskabsplanen er at sikre, at normaldriften genoptages hurtigst muligt i tilfælde af en krise. De lokale organisatoriske enheder har ansvaret for nødprocedurer i den mellemliggende periode.

Akut Medicinsk Koordinationscenter (AMK) varetager den operationelle ledelse af den samlede sundhedsfaglige indsats i regionen i forbindelse med større ulykker og kriser. AMK og CIMT koordinerer og prioriterer indsatsen i it-beredskabssituationer.

## 10. Sikkerhedskultur

Medarbejdernes viden og adfærd i dagligdagen har stor betydning for regionens samlede informationssikkerhed. Derfor skal alle medarbejdere i regionen kende og efterleve informationssikkerhedspolitikken samt de retningslinjer, vejledninger, instrukser m.m., som er relevante i forhold til den enkeltes funktion, rolle og arbejdsopgaver. Til dette formål har Region Hovedstaden et uddannelses- og træningsprogram for informationssikkerhed, som sikrer, at medarbejderne er bevidste om deres rolle og ansvar i sikkerhedsarbejdet og ved,

hvad de skal gøre i konkrete situationer. Programmet udgør samtidig det strategiske grundlag for en sammenhængende indsats med at højne sikkerhedskulturen i Region Hovedstaden. Det er de organisatoriske enheder og linjeledelsens ansvar, at medarbejderne gennemfører uddannelses- og træningsaktiviteterne og i deres daglige arbejde bidrager til en god sikkerhedskultur i regionen.

## 11. Dispensation

I nogle tilfælde kan der være behov for at afvige fra regionens politikker og retningslinjer for informationssikkerhed og databeskyttelse. Til at håndtere dette har regionen etableret en formel dispensationsprocedure, som er forankret i Sektion for Informationssikkerhed i Center for IT og Medicoteknologi (CIMT). Dispensationsproceduren er med til at sikre, at konkrete risici relateret til afvigelsen vurderes og dispensationen godkendes på rette ledelsesniveau.

## 12. Sanktioner

Brud på informationssikkerhedspolitikken eller deraf afledte retningslinjer og vejledninger er underlagt de sædvanlige ansættelsesretlige sanktioner, ligesom brud efter omstændighederne kan anmeldes til politiet.

## 13. Godkendelse og revision

Region Hovedstadens informationssikkerhedspolitik forvaltes af Sektion for Informationssikkerhed, som har ansvar for opfølgning og revision. Revision skal ske løbende og minimum én gang årligt.

Region Hovedstadens informationssikkerhedspolitik godkendes af regionsrådet i Region Hovedstaden og træder i kraft samme dato. Redaktionelle ændringer, som ikke ændrer grundlæggende ved informationssikkerhedspolitikken kan dog godkendes på administrativt niveau jf. Region Hovedstadens styringsmodel for informationssikkerhed og databeskyttelse. Tilsvarende gælder ændringer affødt af regionsrådets beslutninger, der medfører, at der skal laves konsekvensrettelser i informationssikkerhedspolitikken.

**For yderligere information, kontakt:**

Sektion for Informationssikkerhed  
Center for IT og Medicoteknologi  
Borgervænget 5  
2100 København Ø

**E-mail:** [Informationssikkerhed@regionh.dk](mailto:Informationssikkerhed@regionh.dk)

**Intranet:** <https://intranet.regionh.dk/regi/it/informationssikkerhed-og-databeskyttelse/>