C-cure – Total Control
Holte Midtpunkt 20, 2.sal
DK-2840 Holte
Tel. +45 4541 1446
Fax. +45 4546 5401
Mail: info@c-cure.dk
Web: www.c-cure.dk

Metoder til beskyttelse af personoplysninger og ordforklaring

Beskyttelse i lagring og transit kan ske via kryptering. Beskyttelse kan også være i form af adgangskontroller, fysiske såvel som logiske adgangsbegrænsninger til data, baseret på enkelte medarbejderes adgange eller en rolle baseret tilgang. Beskyttelse af personoplysninger kan også være at forhindre at data utilsigtet forlader virksomheden, f.eks. ved begrænsning eller logning af brugen af eksterne medier, USB nøgler mm. Eller via et specifikt Data Leakage Prevention system (DLP) der monitorerer typer af data og forhindrer at de kopieres eller forlader virksomhedens netværk. Der findes også løsninger der forvansker eller anonymiserer bestemte typer af data før de f.eks. bliver sendt via e-mail (Data Redaction)

Data retention period
Den periode data opbevares i som en del af virksomhedens backup løsning

Personoplysninger
Dækker over alle oplysninger der hidrører en fysisk person

Personfølsomme data
Dækker over særligt følsomme data, der f.eks. kan misbruges til identitets tyveri. Personfølsomme data kan være forskelligt defineret i forskellige lande. CPR nummeret er at anse for en personfølsom oplysning, i modsætning til en bopæls adresse, der dog i nogle tilfælde kan være at anse for personfølsom hvis datasubjektet f.eks. har hemmelig adresse.

Personhenførbare data
Alle data der kan henføres til en person. Dette gælder også data der er mere eller mindre offentlige. F.eks. er oplysninger om at datasubjektet ejer en bestemt bil, at regne for personhenførbare data. Ligeledes at der er købt en bestemt vare, så f.eks. en faktura er personhenførbar. Køb af f.eks. medicin (som jo også bare er en vare) vil være personfølsomme oplysninger da de indirekte kan kædes med helbreds oplysninger.

Compliance
Overholdelse af regler; efterlevelse af retningslinjer. Virksomheder bør overholde dels de interne regler fra sikkerhedspolitikker, dels de eksterne krav der måtte være indenfor deres forretningsområde, lovgivninger nationalt og internationalt

ISO27001
Standard til definering af et Information Security Management System. Indeholder en række punkter som en virksomhed bør medtage i deres samlede sikkerhedstiltag, rettet mod ledelsen i en virksomhed og knytter sig til compliance der sikrer overholdelsen. Der findes flere systemer der dels kan checke den tekniske compliance i en virksomhed og dels understøtte arbejdet med ISO27000 standarderne.

ISO27002
Mere detaljeret checkliste der knytter sig til ISO27001 og er af mere teknisk detaljeret karakter

GDPR
General Data Protection Regulation

IP
Internet Protocol

Cookie
Lille tekst fil som websites kan gemme på en besøgendes pc, så man genkendes næste gang man besøger websitet. Tekst filen er i sig selv uskadelig og kan kun læses af det website der selv oprettede den. Bruges dog også på tværs af websites i reklamebannere, hvor det samme reklamefirma kan benytte cookies til at målrette reklamer til den samme bruger over tid. Plug-ins til browsere, konfigurering og antivirus løsninger begrænser brugen af cookies, der dog kan være nødvendige f.eks. til at foretage indkøb på nettet.

RFID
Radio Frequence Identification. Lille radiosender og modtager der bruges f.eks. tøj, varer i et supermarked (tyverisikring) og nyere

C-cure – Total Control
Holte Midtpunkt 20, 2.sal
DK-2840 Holte
Tel. +45 4541 1446
Fax. +45 4546 5401
Mail: info@c-cure.dk
Web: www.c-cure.dk

kredit kort, hvor kontakt løs betaling kan finde sted. Beskyttelse mod en sådan teknologi foregår bedst ved fysisk at sørge for at radio frekvenserne indkapsles. Da det er svage signaler kan dette gøres med alm. metalfolie (sølvpapir).

Forensics
Retsvidenskab. I computer forensics, efterforskning af hændelser i et IT miljø, er det vigtigt at bevis sikre på den rigtige måde, bl.a. ved at følge "Chain of custody". Politiet eller særlige IT sikkerhedsfirmaer vil kunne være behjælpelige med at bevis sikre på en måde der kan bruges i en retsag.

ISMS
Information Security Management System. Samlet betegnelse for en virksomheds informations sikkerheds tiltag, politikker mm, f.eks. baseret på ISO 27000 standarderne.

SOP
I eksemplet: Standard Operating Procedure

Kryptering af data
Under kommunikation og dataopsamling af personhenførbar data, så er det et krav for virksomheden at sikre at disse data er krypteret. Løsninger og teknologier kan assistere virksomheden til at få kontrollen over data flow, adgange (Separation of duties) og data opbevaring effektivt og brugervenligt.

Anvendelse:

- SMS, mail og internet kommunikation
- Adgange (F.eks. VPN til medarbejder der arbejder fra usikre netværk)
- Datalagring, HDD/USBdisk eller backup instanser
- Fildeling
- VOIP

Formål:
Data skal opbevares forsvarligt under benyttelse af krypterings teknologier, der gør det muligt at begrænse adgangen til dataene ved f.eks. at anvende algoritmer, der gør det overskueligt at kryptere, men ekstremt vanskeligt, for de der ikke har krypteringsnøglen, at dekryptere. Kryptering og digital signering kan bidrage til at opretholde konfidentialiteten og integriteten af ens data, samt validere og autentificere sender og modtager.

Typiske krypterings former

- Symmetrisk kryptering (hemmelig nøglekryptering):

Den ældste teknik for nøglekryptering (f.eks. AES). Hvor den samme nøgle anvendes til at kryptere og dekryptere dataene. Det kan f.eks. være kryptering af en zip fil hvor samme nøgle værdi defineres til at kryptere og dekryptere.
Symmetrisk kryptering er den mest effektive til større mængder data, men kræver at der for hver kryptering skabes en unik nøgle der skal hemmeligholdes både af den der krypterer data og den der skal dekryptere dem. Det er den samme nøgle der bruges til kryptering og dekryptering, og der skal derfor være en forudgående hemmelig nøgleudveksling hvis to parter skal kryptere trafikken over et netværk. For nøgle udveksling til brug for hemmelig nøgle kryptering benyttes offentlig nøgle (asymetrisk) kryptering.

- Asymmetrisk kryptering (offentlig nøglekryptering):

Offentlig nøgle (asymmetrisk) kryptering benyttes til bl.a. nøgleudveksling i Hemmelignøgle systemer. Offentlig nøgle systemer er baseret på nogle matematiske principper der gør at en dekrypterings nøgle er forskellig for en krypterings nøgle, så den ene nøgle ikke kan udledes fra den anden. Kryptering foregår derfor via opslag i et centralt register efter den offentlige nøgle (som en slags telefon bog). Alle kan kryptere til en bestemt virksomhed, men kun den der har den private nøgle kan dekryptere. Selve krypterings algoritmen er beregningsmæssig tung i forhold til hemmelignøgle kryptering, og derfor benyttes offentlig nøgle kryptering typisk til at kryptere og transportere nøgler til brug i hemmelignøgle systemer. Benyttes også til digital signatur (certifikater, bevis for identitet, digital underskrift på aftaler, uafviselighed)
Teknologien (f.eks. RSA) anvender en offentlig nøgle til at kryptere data og en privat nøgle til at dekryptere. Derfor kan offentlige nøgler distribueres offentligt og kendskabet til den private nøgle kan dekryptere dataene. Alle kan derfor sende dig data via virksomhedens private nøgle, men kun virksomheden kan dekryptere dataene.

C-cure – Total Control
Holte Midtpunkt 20, 2.sal
DK-2840 Holte
Tel. +45 4541 1446
Fax. +45 4546 5401
Mail: info@c-cure.dk
Web: www.c-cure.dk

Certifikat baseret kryptering
Certifikater. Personlige certifikater, medarbejder og virksomheds certifikater benyttes til digital signatur af dokumenter, udstedes i dag af Nets der kontrollerer DanId der står for NemId løsningen. Server certifikater udstedes enten af virksomhederne selv eller af særlige Certificate Authorities (CA)
Certifikat baseret kryptering er et system, hvor en godkendt certifikat autoritet, udsteder ID-baseret kryptografi. Certifikatet indeholder oplysninger omkring den offentlige nøgle, samt udsteder informationer, anvendelsen og andet metadata. Anvendes bl.a. af Exchange servere, webservere og webapplikationer osv. til at validerer en sikker forbindelse og udveksling af data mellem sender og modtager. Teknologien er kort forklaret en måde til at sikre og validere kommunikation og data mellem sender og modtager.

Digital signatur.
Benyttes til digitalt at underskrive et dokument eller en aftale. Kan også benyttes af f.eks. websteder til at verificere webstedets identitet og / eller til at kryptere data

Access Control - adgangskontrol
Kan foregå som fysisk adgangskontrol eller logisk adgangskontrol. Døre med nøgler, kodeord eller begrænsninger i hvem der må og kan tilgå data eller steder, hvornår og hvordan.

Autorisation
Rettigheder til at se eller tilgå data. Rettigheder kan tildeles på forskellige niveauer, f.eks. på brugerniveau til den enkelte medarbejder eller rolle baseret, hvor bestemte grupper har adgang til bestemte data. Autorisation til dataadgang bør begrænses til dem der har et legitimt behov for data. Dataadgang kan reguleres f.eks. af lovgivning udover EU Persondataforordningen. Bl.a. er der regler for at løn eller andre personlige oplysninger internt i en virksomhed i Danmark ikke må kunne tilgås af andre, end de den nødvendige ledelse og medarbejdere der håndterer løndata. IT administratorer må f.eks. ikke kunne have adgang til løninformationer.
Fysiske og logiske adgangskontroller sættes i værk for at sikre autorisationen, der kombineres med autentifisering, der tilsikrer at det er den rigtige medarbejder der tilgår data. Autorisering kan foregå på database niveau, via Access Control Lists på fil niveau som en del af operativ systemet, via Active Directory el. lign. Der kan være krav om logning af hvem der har tilgået data og hvornår.

Autentificering
Identificering af brugere kan foregå via simpelt brugernavn og password (noget man ” kender”), med en fysisk nøgle (noget man ”har”) eller som en kombination af to eller flere faktorer, f.eks. både noget man kender f.eks. passwords, noget man har f.eks. en fysisk nøgle, en engangskode, en kode genereret af noget man er i besiddelse af, f.eks. koder genereret af et token eller en app på ens egen mobil telefon. Disse kan så yderligere kombineres med andre faktorer, f.eks. at adgangen kun må ske fra et bestemt netværk, fra en specifik session eller fra bestemte IP adresser. Der findes 2 faktor og multifaktor løsninger der kan automatisere denne form for sikkerhed, der går ud over et simpelt brugernavn / password.
Logning
I mange tilfælde kan det være nødvendigt at logge medarbejderes adgang til f.eks. personfølsomme oplysninger. Dels for at forhindre misbrug men også for at dokumentere at gældende lovgivning og / eller compliance er overholdt. Logningens karakter afhænger af behovet. Dog skal det altid tilsikres at der logges, så det kan spores til en enkelt medarbejder og ikke bare til en generisk brugerkonto, f.eks. Administrator. Det skal også sikres at en medarbejder med adgang til data, ikke også har adgang til at slette eller rette i logfiler, der vedrører brugerens eget login. En begrænsning i en sådan adgang er et generelt princip, der baserer sig på ”separation of duties”.

Separation of duties
Generelt princip om at adskille arbejdsområder, så en medarbejder kontrollerer en andens arbejde for at sikre mod potentielt svindel.

Pseudonymisering
Erstatning af direkte personhenførbarhed med inddirekte. F.eks. at en patient i et system ikke står opført med navn og CPR nummer men blot med et løbenummer der refererer til et andet system hvor direkte personoplysninger fremgår. Kan også dække over at datasubjektet selv vælger et pseudonym, f.eks. et brugernavn, kælenavn eller andet.

Anonymisering
Alle personhenførbare data anonymiseres til noget der ikke kan føres tilbage til datasubjektet. Hvis der i en begrænset mængde data vil kunne identificeres enkelt individer på trods af anonymiseringen, f.eks. ved sammenlægning af data. Data Redaction eller DLP løsninger vil kunne anonymisere eller forhindre visse typer af data læk.

C-cure – Total Control
Holte Midtpunkt 20, 2.sal
DK-2840 Holte
Tel. +45 4541 1446
Fax. +45 4546 5401
Mail: info@c-cure.dk
Web: www.c-cure.dk

DLP – Data Leakage Prevention
System til begrænsning af data der kan forlade virksomheden. Typisk holdes øje med bestemte typer data (f.eks. kredit kort numre, CPR numre eller andre følsomme data)

Logning og auditering
Formål: Opsamle data til videre behandling som f.eks. bevissikring, fejlsøgning og dokumentation.
I forlængelse af Adgangskontrol & adgangsbegrænsning er det essentielt at virksomheden kan monitorere og påvise brud på integriteten og konfidentialitet af data ved at logge/opsamle data på mulige ændringer og indsigt i systemer og data. Under et brud er logning og auditering med til at vise præcis hvordan og af hvem data er blevet eksponeret, men på den anden side også til for at sikre at de pågældende systemer ikke har været kompromitteret. Dermed sagt kan det defineres som løsninger der laver aktiv bevisførelse og sikring.

Data destruktion
Formål: Bortskaffelse af data logisk eller fysisk ved destruktion af harddisk

- Logisk
  Værktøjer kan anvendes i forbindelse med data destruktion, hvor man fremadrettet ønsker at anvende hardwaren i andre henseender. Der findes forskellige teknologier til at slette og overskrive data, så tidligere data sættes i en ubrugelig state, som ikke er mulige at genskabe.
- Fysisk
  Skal man kunne sikre sig endegyldigt at data ikke kan genskabes, kan det være nødvendigt at destruere harddisk og hardware. Skal data destrueres på en sådan måde, så er det vigtigt at hardwaren står tilbage som fuldstændig ubrugelig. Det er derfor ikke nok at anvende en hammer, men komponenterne skal gerne være i den dårligste forfatning muligt.

Backup
Backup løsninger findes i mange forskellige udgaver og til forskellige medier. Fælles for dem alle er at formålet er at være i kontrol med data og kunne genskabe data indenfor en estimeret tidsramme.
Virksomheden skal sikre at der forefindes en backup til genskabelse af data inden for en estimeret tidsramme. Data kan i nogle løsninger krypteres. I tilfælde af opbevaring hos ekstern tredjepart, skal det tilsikres at backupppen kun vil være tilgængelig for den data ansvarlige. Backupløsninger til Cloud eller on-premise kan effektivisere og automatisere virksomhedens omgang med data. I løsningerne vil det være muligt at definere adgange og praktisere separation of duties. Nogle backup løsninger giver kun mulighed for en fuld genskabelse af data, ikke en delvis genskabelse. Dette kan give virksomhederne en udfordring hvis et datasubjekt beder om at data slettes, og det ikke teknisk er muligt at slette eller identificere enkelte data inde i backuppen.

Data Leakage Prevention
Formål: Tiltag for at forhindre sensibelt data i at forlade virksomheden.
Der findes adskillige løsninger på markedet, som contentfiltre, firewalls osv. der kan hjælpe virksomheden med at kontrollere hvilke data der forlader virksomheden. I filtrene kan der opsættes politikker som forhindrer medarbejdere i f.eks. at inkluderer CPR-numre, årsregnskaber, databaser m.m. i udgående mails.

Data Portabilitet
Formål: Her handler det igen om kontrol af virksomhedens data samtidig med en funktionel bevægelig arbejdsstyrke.
Ved flytning, opbevaring og deling af data mellem medarbejdere, f.eks. på mobilen, fildeling og flytbare-enheder, så findes der centralt administrerede løsninger der kan begrænse virksomhedens arbejdsbelastning, ved at implementere politikker om slettefrister, kryptering, adgange, deling m.m.

Fysisk adgangsbegrænsning
Formål: Dæmme op for fysisk adgang for uvedkommende til virksomhedens data og IT udstyr.
Har virksomheden implementeret fysisk perimeter sikkerhed, som brug af adgangskort, medarbejder awareness, definerede fysiske arbejdsområder, aflåst server & kommunikations område, lås på vinduer og døre ved pauser osv. Der er konsulentvirksomheder der implementerer og vurderer fysisk sikkerhed til virksomheder. Der vil blive under dække blive efterprøvet hvorvidt det er muligt at tilegne sig adgang til virksomhedens computere eller andet der kan give adgang og kompromittere virksomheden.

C-cure – Total Control
Holte Midtpunkt 20, 2.sal
DK-2840 Holte
Tel. +45 4541 1446
Fax. +45 4546 5401
Mail: info@c-cure.dk
Web: www.c-cure.dk

Logisk adgangsbegrænsning
Formål: Forhindre ekstern og intern uautoriseret eller skadelig adgang til data.
Anvendes der teknologier som beskytter slutbrugeren, som slutbrugersikkerhed(Antivirus), password politikker, begrænsning af brugerrettigheder, backups. Virksomheden skal sikre at de løsninger som anvendes til perimeter- og slutbruger sikkerhed indeholder de teknologier, der er nødvendig for at dæmme op for tidens trusselsbillede. Det kan f.eks. være Next generation firewalls, der har avanceret scanning af teknologiernes forskellige lag og avanceret beskyttelse imod nye trusler og avancerede angreb.

Privacy by design
Formål: Allerede i opstartsfasen af et projekt eller tiltag at tage udgangspunkt i at personfølsomdata beskyttes.
Betyder at virksomheder skal beskytte personoplysninger og personhenførbart data i teknologiske tiltag, softwaredesign og forretningsstrategier fra projekternes start. Fremadrettet skal Privacy by Design og Privacy by Default være indarbejdet som standard.

Privacy by default
Formål: En standard procedure for opbevaring og afgrænset behandling af personfølsom data.
Betyder at virksomheden skal indføre procedure, der som standard sikrer behandling og opbevaring med personfølsomdata, og at der kun behandles den nødvendige data for virksomhedens formål. Fremadrettet skal Privacy by Design og Privacy by Default være indarbejdet som standard.

PIA- Privacy Impact Assessment
Formål: At sikre datasubjektet og vurdere påvirkning og mulig risiko for behandling af dennes data hos virksomheden.
En PIA er en vurdering af påvirkning og mulig risiko, set fra datasubjektet individuelle synspunkt, ved behandling eller opbevaring hos en instans som f.eks. en virksomhed.

Fildeling
Virksomheders behov for fildeling med 3. parter skal sikres på linie med øvrige data. Kryptering under transport og opbevaring af data skal sikres. Det skal bemærkes at kryptering der er foranlediget af leverandøren af fildelings tjenesten, hvor virksomheden ikke selv definerer og opbevarer krypterings nøglen, ikke er at betragte som egentlig kryptering da 3. part jo har adgang til data.

Har man yderligere spørgsmål står C-cure selvfølgelig til rådighed.