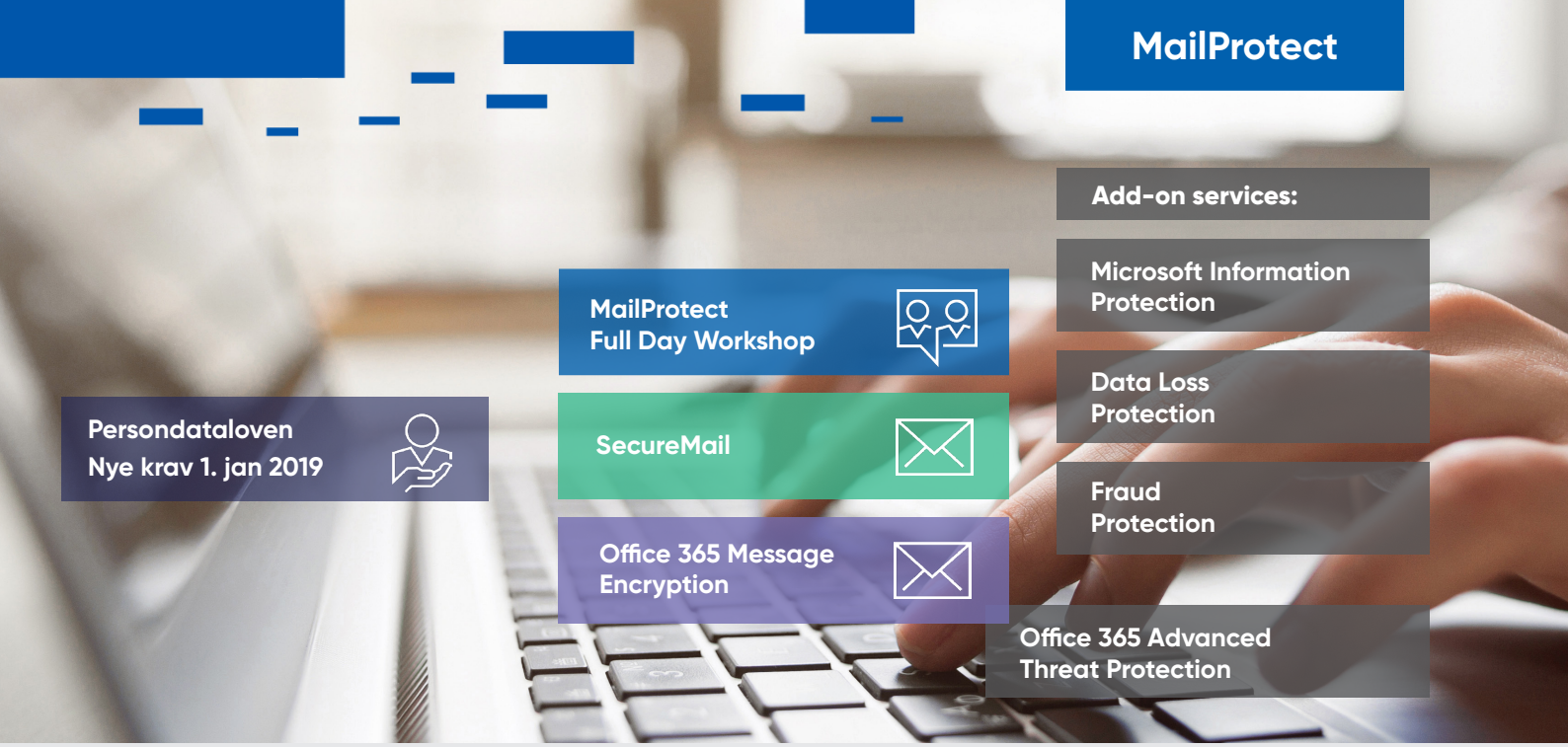


# Kom hele vejen rundt om mailsikkerheden

## Skærpede krav fra Datatilsynet på vej

I kølvandet på GDPR skærper Datatilsynet kravene til private virksomheders håndtering af fortrolige og personfølsomme oplysninger. Offentlige myndigheder har igennem flere år været pålagt at kryptere e-mails med personlige oplysninger, men nu er turen også kommet til de private virksomheder.

Tidligere har det blot været en anbefaling, at private virksomheder krypterer borgernes personfølsomme oplysninger. Men fra **1. januar 2019** bliver Datatilsynets anbefaling ændret til et ufravigeligt krav, der omfatter både store og små virksomheder samt organisationer.

Efter nytår vil Datatilsynet derfor kunne straffe jeres virksomhed med påbud, forbud eller bøder, hvis ikke I kan dokumentere, at I i passende grad har beskyttet borgernes personfølsomme oplysninger.

Fremadrettet bliver det derfor afgørende at sikre, at indholdet i en e-mail først kan blive afkodet, når den rette modtager åbner den. Som virksomhed vil I få behov for:

- Beskyttelse af personfølsomme data under transport
- Mulighed for at håndtere fx "retten til at blive glemt"
- Dokumentation af hvem, der har afsendt e-mail og validering af indholdet
- Mulighed for leverance af digital post til e-boks, virk.dk og borger.dk

## MailProtect Full Day Workshop

Vi kan hjælpe jer godt i gang på en workshop, hvor vi tager udgangspunkt i lovgivningen og de nye krav, der kommer til at gælde pr. 1. januar 2019.

I vil blive præsenteret for løsningsmuligheder, der vil passe til jeres it-setup. Hvis I har behov for det, kan vi også sørge for grundopsætningen af den sikre e-mailløsning. Her vil vi ikke bare kunne stå for opsætningen på de krypteringsløsninger, som vi selv leverer, men også håndtere andre løsninger, som kunne være relevante for jer.

## SecureMail - automatisk kryptering og dekryptering

En af de løsninger, vi kan hjælpe jer med, er SecureMail. Med den får I mailfiltrering, signering og kryptering i én og samme løsning.

Ved benyttelse af SecureMail vil løsningen automatisk ved afsendelse af en e-mail kontrollere hvorvidt modtageradressen kan modtage krypterede e-mails eller ej. Er det tilfældet vil SecureMail derefter automatisk kryptere e-mailen med modtagerens certifikat og tilsvarende signere den med afsenderens. Det hele sker uden indblanding fra den pågældende medarbejder. SecureMail krypterer automatisk, når det kan lade sig gøre, stiller en fuld log af korrespondancen til rådighed og eliminerer manuelle fejlkilder.

**Modtagelse af digital post**
Digital Post/e-Boks er en af myndighedernes sikre kommunikationsformer, i form af virk.dk til virksomheder og borger.dk til borgere. SecureMail kan integreres problemfrit med virksomhedens digitale postkasse på virk.dk og på den måde undgår den enkelte medarbejder at skulle gå via virk.dk for at modtage henvendelser fra det offentlige.

SecureMail sørger for, at alle e-mails til den digitale postkasse bliver sikkert videresendt til virksomhedens eget mailsystem og medarbejderens egen mailklient, fx Outlook - og besvares derfra, som en sikker og krypteret e-mail. Jeres medarbejdere behøver ikke at bekymre sig om login på virk.dk, videresendelse eller arkivering af beskeder fra det offentlige.

Og sidst, men ikke mindst, er det sikkert at videresende og besvare fortrolige eller personfølsomme oplysninger til både kolleger, eksterne samarbejdspartnere og kunder. Den enkelte medarbejder vil derfor ikke opleve væsentlige ændringer i sin måde at sende og modtage e-mails på.

**Aflever via virk.dk og borger.dk**
Med SecureMail er det muligt at sende sikkert til alle danskere over 15 år med et CPR-nummer, samt alle danske virksomheder med et CVR-nummer. Det kræver blot som tillæg en afleveringsaftale med e-Boks, som vi fordelagtigt kan tilbyde og hjælpe med at sætte op.

## Office 365 Message Encryption

En anden mulighed er Office 365 Message Encryption. Office 365 Message Encryption gør det nemt at sende krypterede e-mails til alle – inden for såvel som uden for jeres organisation. Løsningen krypterer hele e-mailens indhold og understøtter validering af modtageren via Office 365 konto, Microsoft konto, Google konto, Yahoo konto, m.fl. Hvis modtageren ikke har nogen af de konti og dermed ikke kan valideres, er det muligt at benytte one-time password. .

En finesse er at e-mails, der er krypteret med Office 365 stadig er søgbare, når e-mailen ligger i Office 365. Modtager kan desuden besvare e-mailen krypteret, også selvom modtageren ikke selv har Office 365. For at få Office 365 Message Encryption skal I have Office 365 Enterprise E3 eller lignende.

For Office 365 Message Encryption gælder, at vores konsulenter kan lave grundopsætningen for jer.

## Add-on services

Udover krypteringsløsningerne tilbyder vi forskellige add-on services med tilhørende konsulentbistand. Add-on bygges oven på de øvrige løsninger. Vi tilbyder et setup, hvor I køber en halvdags workshop, og hvor efterfølgende opsætning og implementering håndteres af vores konsulenter på T&M basis.

**Advanced Threat Protection (ATP)**
ATP er en tilføjelse til sikkerhedsprodukterne i Office 365. Advanced Threat Protection hjælper med at forsvare jeres brugere mod sofistikerede trusler, der er skjult i e-mails, vedhæftede filer og links.

**Microsoft Information Protection (MIP)**
MIP giver jer mulighed for at kryptere dokumenter, så de ikke kan læses af uvedkommende, uanset hvordan dokumenterne har forladt virksomheden. Når en medarbejder forlader virksomheden, vil vedkommende heller ikke kunne læse data, selv om de er medbragt på en USB-nøgle. Der er mulighed for manuel eller automatiseret label af dokumenter, så de bliver grupperet ud fra et bestemt regelsæt. Data kan klassificeres ud fra tekstmønstre - fx graden af følsomhed - og derved bedre understøtte "retten til at blive glemt".

**Data Loss Protection (DLP)**
DLP forhindrer tab eller videregivelse af følsomme eller kritiske oplysninger. Teknologien identificerer tilfælde, hvor der kan være en aktiv lækage af følsomme data, enten via advarsel eller forebyggende foranstaltninger. Følsomme data vil blive identificeret på tværs af lokationer og platforme, som fx Exchange, Sharepoint og Onedrive.

DLP sørger altså for, at data er tilgængelige hele tiden, men samtidigt er sikret mod uhensigtsmæssig og ulovlig deling. I opnår derfor compliance, uden at jeres arbejdsgange påvirkes negativt.

**Fraud Protection (SPF / DKIM / DMARC)**
**SPF** (Sender Policy Framework) er en åben standard, der angiver en metode til at forhindre forfalskning af afsenders adresse. SPF gør det muligt for jer at identificere jeres domænes godkendte kilder til e-mails og forhindrer, at uautoriserede kilder sender tusindvis af ulovlige e-mails fra jeres domæne.
**DKIM-signering** (DomainKeys Identified Mail) af domæner i DNS bygger på en nøglestruktur, der sikrer, at e-mails kommer fra den rigtige afsender, og at indholdet ikke er ændret undervejs.
**DMARC** (Domain-based Message Authentication, Reporting and Conformance) knytter SPF og DKIM sammen og gør det dermed muligt at overvåge og styre jeres virksomheds mailflow. I får langt større sikkerhed mht. anvendelsen af virksomhedens domæner og kan hurtigt identificere mailservere, der sender på vegne af eget domæne.