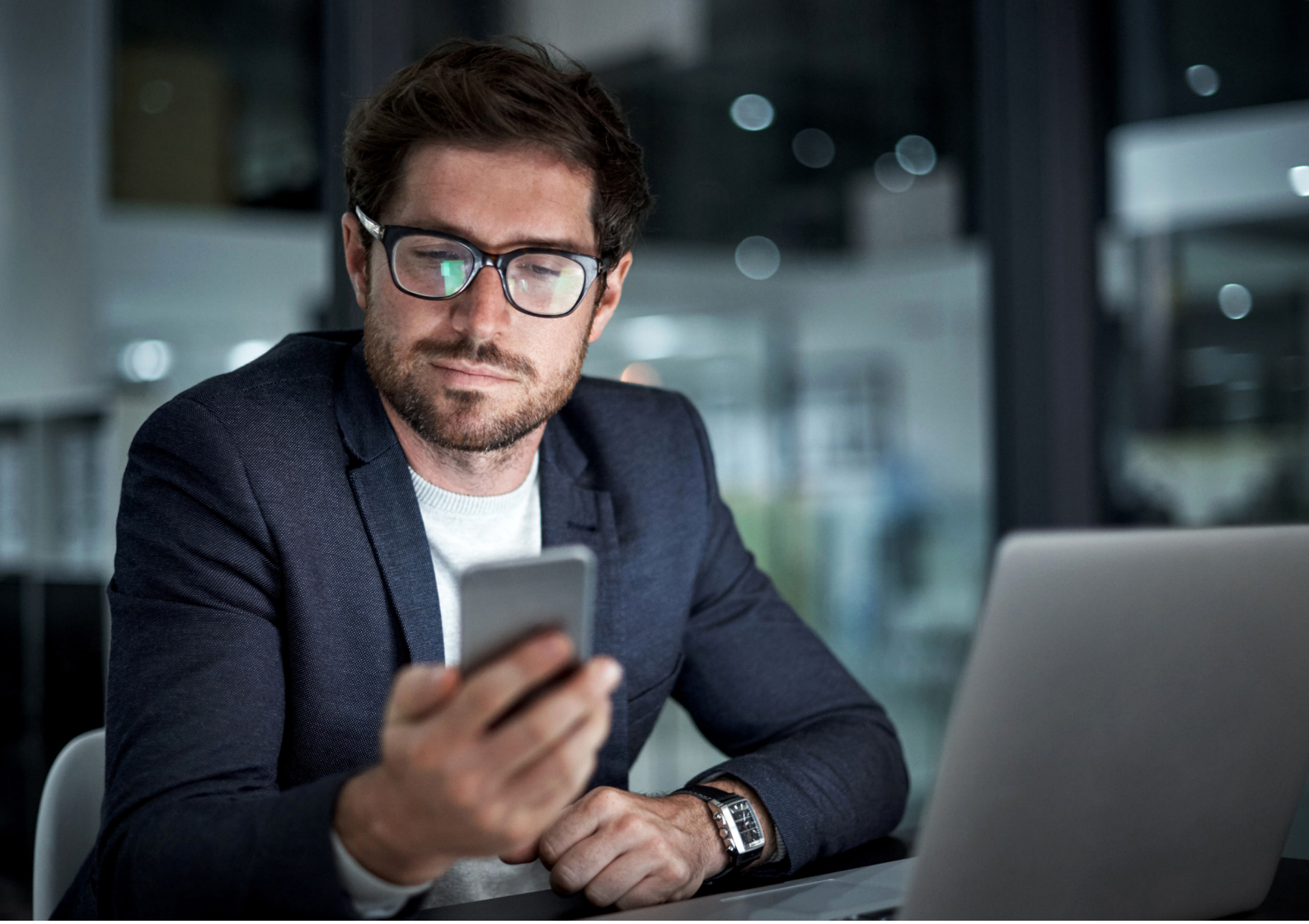

GUIDE

3 trin til beskyttelse af virksomhedsdata på arbejdstelefonen

TELE IT

Har du styr på de persondata, der ligger på dine medarbejderes telefoner og tablets?

Mobile enheder kan være tikkende GDPR-bomber – især hvis medarbejderne benytter den samme enhed til arbejde og i privat regi.

I denne guide præsenterer vi 3 simple måder, hvorpå du kan sikre, at både du og dine medarbejdere overholder GDPR-kravene på arbejdstelefonen og andre mobile enheder.

#1 Uddan og test dine medarbejdere

En af de helt store syndere i relation til GDPR er, at medarbejderne utilsigtet deler fortrolige persondata via deres mobile enheder. Det kan f.eks. ske, når medarbejderne ukritisk downloader apps, der "høster" de personfølsomme data, som ligger på enheden.

Men utilsigtet deling er ikke den eneste sikkerhedsrisiko. Også udefrakommende trusler som virus og malware-angreb kan spore og indsamle persondata, hvilket selvfølgelig også falder under GDPR.

I sidste ende er det altid mennesker – altså dine medarbejdere – der er det svageste led, når det kommer til IT-sikkerhed.

Uddannelse af medarbejderne er derfor alfa og omega. Medarbejderne skal blive helt klar over risikoen og klædes bedre på til at sikre deres telefoner. Samtidig anbefaler vi også, at I phishing tester jeres medarbejdere og derefter tilbyder uddannelse til dem, der har den mest risikable adfærd.

Det er vigtigt at øge bevidstheden om sikkerhedsrisici – særligt blandt medarbejdere, som kan tilgå data eksternt fra forskellige enheder og netværk. Sørg for, at dine medarbejdere løbende får information om, hvordan de kan beskytte sig, og påmindelser om at installere antivirus-software, opdatere adgangskoder og opgradere sikkerheden, så de ikke utilsigtet deler persondata med tredjepart.

Det vil altid være virksomhedens ansvar, at der er styr på data, og det er derfor virksomhedens ansvar at både teknik og uddannelse er i orden.

Kontakt
www.teleit.dk
+45 7023 0373
info@teleit.dk

#2 Lav fælles retningslinjer

Listen over mulige foranstaltninger er lang, og det er ikke nødvendigvis alle, der er lige gavnlige eller nødvendige for alle.

Først og fremmest handler det om at minimere risikoen for GDPR-overtrædelse – og hvor der er persondata, er der risiko for overtrædelse.

Så hvilke foranstaltninger er de bedste for jer og bør være et krav, at alle implementerer på deres enheder?

Dernæst handler det om at skabe fælles retningslinjer omhandlende persondata på mobile enheder.

- Hvor ofte skal adgangskoder opdateres?
- Hvor stærke skal kodeord være?
- Hvilken antivirus-software og sikkerhedsløsninger skal installeres?
- Osv.

Bøderne for overtrædelser af GDPR kan være op til 4% af den globale omsætning. Den eneste undtagelse er, hvis virksomheden kan bevise, at dataene var ordentligt krypterede.

Derfor bør I også implementere processer og software til at kryptere drev og filer, så medarbejderne skal anvende et kodeord for at tilgå og dekryptere dataene. På den måde 'tvinger' man medarbejderne til at få for vane at bruge kodeord til alt.

#3 Implementér Mobile Device Management

Ovenstående trin er gode i forhold til at få medarbejderne med ombord og etablere gode vaner. Men som sagt er mennesker bare mennesker – og mennesker laver fejl.

Og hvordan forholder vi os til det?

Mens de to første trin er vigtige, så efterleves GDPR ikke, hvis I ikke har en Mobile Device Management-løsning til styring og kontrol af enhederne og den persondata, der ligger på dem.

MDM er en løsning, der gør det muligt at håndtere og sikre alle virksomhedens mobile enheder fra ét, centralt system. MDM giver administratoren overblik og kontrol, og med MDM får virksomheden vished om, at medarbejderne ikke henter risikable apps, der potentielt kan skade virksomheden.

Med MDM kan du samtidig sikre GDPR-compliance i forhold til både følsomme og personfølsomme data, som gemmer sig på medarbejderne telefoner. Derudover sparer du tid med MDM, da MDM automatiserer en række processer omkring opsætning af enheder samt generel management og support af dem.

5 konkrete udbytter med en MDM-løsning

1. Virksomheden får administrationsretten og kontrollen tilbage
2. Privat- og virksomhedsrelaterede data bliver adskilt (GDPR)
3. Stor tidsbesparelse på opsætning og support af de mobile enheder
4. Overblik over enheder og incidents
5. Remote sletning (wipe enheden, hvis den tabes eller stjæles)

Hos TELE IT er vi certificerede specialister i IT-sikkerhed, netværk og tele-løsninger.

Vi arbejder med komplekse IT- og kommunikationsløsninger, og vi kan hjælpe dig med at få 100% styr på din IT-infrastruktur. Vores stærke partnerskaber sikrer, at de ydelser og produkter vi benytter, er af den bedste kvalitet, der findes på markedet.

Udover vores stærke partnerskaber har vi samlet nogle af Danmarks dygtigste systemkonsulenter, der altid er ajour med, hvad der foregår på markedet.

TELE IT

Kontakt
www.teleit.dk
+45 7023 0373
info@teleit.dk