IT og DATA Sikkerhedspolitik i forbindelse med persondata

Sikkerhedspolitik i forbindelse med Personaleadministration, Kunder, Patienter, Leverandører

Når vi i Rademacher's Orthodontiske Laboratorium ApS (omtales i følgende som ROL) behandler oplysninger om vores Medarbejdere / Patienter / Kunder / Leverandører sker dette under overholdelse af databeskyttelsesreglerne, herunder kravene om datasikkerhed.

- Data anvendes kun til det formål som de er indsamlet til
- Data kontrolleres med stor IT-sikkerhed for at forhindre utilsigtet adgang og spredning
- Data er korrekte og informationer retvisende
- Data slettes efter faste retningslinjer for hvornår disse kan / skal slettes
- Data skal kunne genskabes uden unødig forsinkelse
- Data kan udleveres til person som de vedrører, hvis dette ønskes af person
- Samtykke indhentes i forbindelse med indsamling / offentliggørelse af billeder / info på virksomhedens hjemmeside / sociale medier eller anden offentlig kommunikation som ikke kommer fra/ offentliggøres af den (de) berørte person (-er) selv.
- Alle i virksomheden er ansvarlig for at sikre en høj datasikkerhed og følge virksomhedens IT-sikkerheds politik
- Alle i virksomheden er ansvarlige for at følge beskrevne procedure og retningslinjer i virksomheden
- Informer STRAKS den dataansvarlige hvis der er konstateret eller mistanke om brud på datasikkerhed
- Virksomheden indberetter alle brud på datasikkerhed, hvis der sker et sikkerhedsbrud, som kræver anmeldelse
- Virksomheden sikre en løbende opfølgning og kontrol med procedure og retningslinjer i forhold til datasikkerhed og efterlevelse af persondataforordningen
- Virksomheden arbejder løbende på at forbedre og vedligeholde datasikkerhed så der anvendes tidssvarende systemer og metoder, og lovgivnings krav overholdes
- Ved anvendelse af ITsystemer, programmer, App´s og andre platforme, sikres det gennem standard indstillinger, at kun personoplysninger, er er nødvendige til et specifikt formål behandles, således at mindst mulig deling af personoplysninger sikres.
- Mulighed for at "anonymisere / pseudonymisering" af personoplysninger på en sådan måde, at disse ikke kan henføres til en bestemt registreret person, vil blive anvendt i den udstrækning det er muligt og relevant i forhold til datas karakter.

Helt overordnet betyder det, at ROL drager omsorg for, at alle personoplysninger i er beskyttet, så ingen oplysninger tilintetgøres, fortabes eller forringes. Samtidig drager virksomheden omsorg for, at ingen oplysninger kommer til uvedkommendes kendskab, misbruges eller behandles i strid med reglerne, samt at det tilstræbes at inden informationer er ukorrekte eller misvisende.

Alle medarbejdere, der håndterer oplysninger om Kolleger / Patienter / Kunder/ Leverandører, har pligt til at overholde følgende regler:

1. Adgangen til oplysninger begrænses til så få personer som muligt. Det er således kun personer, der har et sagligt behov for det, der har adgang til oplysningerne.
   I forhold til personale oplysninger er adgang begrænset til virksomhedens øverste ledelse.

2. De medarbejdere, der håndterer kollegers personoplysninger, modtager instruktion og oplæring i, hvordan de skal håndtere og beskytte oplysningerne, og hvad oplysningerne må bruges til. Medarbejder har pligt til at følge disse instrukser og deltage i oplæringen

3. Personoplysninger (alle), der findes i papirform, fx i kartoteker og ringbind, skal opbevares aflåst, når de ikke er i brug. Når oplysningerne skal smides ud, skal de makuleres.

4. Hvis du håndterer elektroniske personaleoplysninger / Patient data / Kunde data / Leverandør data, får du udleveret en kode, der giver adgang til de oplysninger som er relevante for opgaver som du er tilknyttet. **Koden er personlig og må under ingen omstændigheder efterlades eller gives videre til andre**. ROL kontrollerer og opdaterer koderne mindst 2 gange om året.

5. ALLE personoplysninger behandles fortroligt og under tavshedspligt.
Personoplysninger som du har adgang til i forbindelse med dit arbejde, skal håndteres således at denne fortrolighed og tavshed ikke brydes. Dette gælder i særligt grad personfølsomme informationer, men er ikke begrænset til dette.

6. ROL registrerer, hvis nogen forgæves har forsøgt at få adgang til virksomhedens IT-systemer med følsomme personoplysninger. Hvis der registreres tre på hinanden følgende forsøg på adgang, blokerer vi for yderligere forsøg.

7. Personoplysninger på bærbare datamedier:
Personaleoplysninger / Patient oplysninger / Kunde oplysninger / Leverandør oplysninger, der er lagret på en USB-nøgle/ ekstern bærbar harddisk, skal beskyttes på en hensigtsmæssig måde. Du skal derfor anvende USB-nøgler/ ekstern bærbar harddisk med adgangskode / kryptering eller opbevare USB-nøgler/ harddisk i aflåst skuffe eller skab.
Tilsvarende gælder andre bærbare datamedier, der indeholder personoplysninger.

8. Du skal låse computeren, når du forlader den.

9. Du skal slukke din computer, når du går hjem.

10. Inden du går hjem, skal du sikre dig, at vinduer er lukkede, døre er låst, og at alarmen er slået til.

11. Der skal være lås på alle mobiltelefoner og bærbare enheder, der synkroniserer mail og kalender.

12. Når dataudstyr, der indeholder personoplysninger, sendes til reparation eller service, og når datamedier kasseres, skal der træffes fornødne foranstaltninger, så personoplysningerne ikke kommer til uvedkommendes kendskab. Det indebærer blandt andet, at datamediet i videst muligt omfang renses for oplysninger, og at der i fornødent omfang tages sikkerhedskopi.
Tilsvarende gælder, hvis dataudstyr stilles til rådighed for en anden medarbejder.
Hvis data ikke kan fjernes ved en reparation (uhensigtsmæssigt), underskrives en tavsheds erklæring med service firma, hvis IT udstyr overlades til ekstern, som får adgang til PC / IT systemets data.

13. Når vi bruger en ekstern databehandler til at håndtere persondata, indgår ROL en skriftlig databehandleraftale med den eksterne databehandler, der sikrer, at gældende regler bliver overholdt. Det gælder for eksempel, hvis vi anvender et eksternt dokumentarkiv, eksternt

lønbureau eller rekrutteringssystem på internettet.

14. Hvis der sker et sikkerhedsbrud, som kræver anmeldelse til Datatilsynet, skal denne anmeldelse ske senest 72 timer, efter at sikkerhedsbruddet er kendt. Der skal ikke ske anmeldelse, hvis sikkerhedsbruddet, hvis det er usandsynligt, at sikkerhedsbruddet har indebåret en risiko for en medarbejders rettigheder. ROL orienterer som udgangspunkt også en medarbejder, hvis et sikkerhedsbrud indebærer høj risiko for medarbejderens rettigheder. ROL sikrer fornøden dokumentation for alle brud på datasikkerheden.

    Sker der et sikkerhedsbrud, skal du derfor straks kontakte Simon Groth, som er den daglige leder så ROL kan foretage en vurdering af sikkerhedsbruddets karakter og iagttage eventuelle forpligtelser efter databeskyttelsesreglerne.

15. ROLhar i fornødent omfang implementeret relevante IT-back-up systemer, således at man rettidigt kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysisk eller teknisk hændelse. Dette har man gjort på følgende måde: Der tages en daglig backup af ordrebogen. De enkelte databaser med digitale scan bliver løbende opdateret med backup i hver digitale platform (Sirona Dentsply og 3shape) Mailsystemet opdateres løbende af vores samarbejdspartner Vestnet. Firmaets hjemmeside varetages af Dandomain.

16. ROL har i fornødent omfang implementeret en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed. Dette har man gjort på følgende måde: Se P 4.19 Persondataforordningen afsnit 4.1.17 Dokumentation – efterprøvning, samt dokument SM 4.19-02 Tjekliste for kontrol af persondatafording.
    Her fremgår det blandt andet, at der min. 1 gang hvert halve år, vil være en efterprøvning og kontrol af de sikkerhedsforanstaltninger som er gældende i virksomheden.

17. Computere skal have en opdateret firewall og viruskontrol installeret, som lever op til passende sikkerhedsmæssige standarder. Dette har man gjort på følgende måde: Vi har installeret McAfee antivirus program på samtlige pc'ere, som løbende bliver opdateret.

18. Andet elektronisk udstyr - tablets/ iPads/ mobiltelefoner skal, hvis der ligger mail eller person data på telefon, sikres med opdateret firewall og viruskontrol.

19. Du må IKKE indlæse NY software / programmer på computer, uden at dette er aftalt med den IT ansvarlige

20. Data gemmes og arkiveres (elektronisk og fysisk) i henhold til retningslinjer som er opstillet af virksomheden.

21. Ved brug af virksomheds e-mail, sikres det at der anvendes "sikker mail", og at person data som sendes via mail / IT ikke "falder i de forkerte hænder"
    (se dokument xxx om brug af sikker mail)

22. Hvis der benyttes hjemmesideformularer, hvor følsomme personoplysninger og personnummer kan indtastes og fremsendes, skal der anvendes kryptering. Dette har man gjort på følgende måde: Simon G. er i gang med at finde en løsning [indsæt beskrivelse].

Regler for e-mail:

Virksomheds mail konto
Medarbejder som får oprettet en VIRKSOMHEDS mailkonto – skal kun anvende denne til virksomheds relaterede arbejdsopgaver, og må være bekendt med at virksomheden har ret til at gennemgå og læse alle mails som ligger i denne mailboks. Både mens medarbejder er ansat i virksomheden, og efter ansættelses forhold er ophørt.

a) Regler for Private mails:
Virksomheden tillader ikke at mailsystem anvendes til private mails.
Alle mails som sendes og modtages via virksomhedens mailsystem betragtes som virksomheds mail.

b) Privat mail konto
Medarbejder som får oprettet en PRIVAT mailkonto, - skal være opmærksom på at denne IKKE må anvendes til virksomheds relaterede opgaver.

c) Private mails – medarbejder har ikke privat mail konto.
Hvis medarbejdere ikke har en mailkonto som er specifikt kun til private mails, SKAL medarbejder oprette en særlig folder til "Private mails". Mails som ligger i medarbejders "Private folder", må IKKE have virksomheds relateret indhold, og må KUN anvendes til rent private anliggender.

Mails må IKKE anvendes til Uetisk, kriminelle eller virksomheds skadelig aktivitet.
Hvis virksomhed har begrundet mistanke om at der er foregået kriminel eller virksomheds skadelig aktivitet via den private mail konto, kan der i særlig tilfælde gives adgang til medarbejders private mail konto.
Hvis det opdages at medarbejder anvender PRIVAT mail konto til virksomheds relaterede opgaver, gives i første omgang en skriftlig advarsel. Konstateres brud på den tiltænkte anvendelse af PRIVAT mail konto gentagende gange, vil dette medføre at PRIVAT mailkonto lukkes for medarbejder.

LINKS i e-mail.
*ALLE medarbejdere som har adgang til en virksomheds oprettet mailkonto, det gælder både en Virksomheds mail og privat mail konto, skal være opmærksomme på **ikke** at klikke på links i mails som der kan være tvivl om er sikre. Mails som modtages fra "ikke kendt" personer, skal vurderes som KRITISKE og links skal bekræftes af afsender inden der klikkes på disse.*

SIKKER MAIL.
I forbindelse med øget sikkerhed, har virksomheden besluttet at der kun må modtages mails – hvor der er person data, som sikker mail, - se I 4.19-04 Brug af sikker mail.
Det er derfor vigtigt at alle relevante medarbejder oprettes med en medarbejder profil, som gør at man kan sikre at mails som sendes / modtages i størst muligt omfang kun modtages fra andre som også anvender sikker mail.

Ved kommunikation med det offentlige anvendes virksomheds ID – Skat og løn.
Medarbejder signatur fra Nets.

Virksomhedens e-boks, anvendes til kommunikation med det offentlige.

Fratrådt medarbejder – e-mail konto.

Når medarbejder forlader arbejdspladsen og ikke længere kan få adgang til mailkonto på arbejdspladsen, vil den aktuelle mailkonto blive forsynet med et "autosvar", med besked om at medarbejder ikke er ansat længere, samt eventuel anden relevant information.

Eventuelle personlige e-mail adresser fjernes hurtigst muligt fra hjemmeside og andre offentligt tilgængelige informations steder.

Medarbejders Private mail konti / private foldere gemmes i op til 12 mdr. efter medarbejder er fratrådt i virksomheden.
Virksomheds mail konti, - fortsætter uden ændringer, og data opbevares i periode som det giver mening af virksomheds hensyn.

Regler for brug af mobil telefon:
Virksomheds brug:
Alle data, som indeholder personfølsomme oplysninger, f.eks. foto af arbejdssedler eller sms'er, skal som udgangspunkt være krypteret. Data skal slettes, så snart de ikke længere benyttes.

Privat brug:
Bliver en mobil anvendt til at overføre data eller som værktøj i forbindelse med en arbejdsopgave, skal disse data slettes igen, så snart de ikke længere anvendes. ROL er i gang med at indarbejde procedurer, som bruges til at følge op på at reglerne overholdes.

Generelt:

Regler for hvordan man begrænser utilsigtet adgang til data:

Standard regler for arbejde med personfølsomme data:

- *Ingen papirer må ligge frit fremme på dit skrivebord, uanset hvad.*
- *Alle papirer på dit skrivebord skal låses væk inden du går hjem.*
- *Papirer til udsmidning skal makuleres og smides i en dertil indrettet boks.*
- *Når du ikke er ved din arbejdsplads, så skal computeren låses*
- *Når arbejder på PC hvor skærm vender ud mod personer som ikke er godkendt til at have adgang til informationer (eks. Skærm i reception, eller kunde område), vær da opmærksom på ikke at have informationer på skærmen, som kan indeholde personfølsomme oplysninger, så disse vises for uvedkommende. Vend skærmen, eller luk ned for det du er i gang med, indtil der er ikke er uvedkommende i nærheden som kan læse med på skærmen.*
- *Mails med personfølsomme oplysninger – slettes hurtigst muligt og senest efter 30 dage. Er der behov for at gemme information (mail / vedhæftede dokumenter), gemmes disse i mapper som de forskellige dokumenter / informationer hører til.*

Regler om TV overvågning:

ROL anvender ikke TV/video-overvågning.

Brug af internet:

Medarbejder som har adgang til internet i forbindelse med arbejde i virksomheden, skal undlade at surfe på internet sider som kan have pornografisk indhold, spil udbyder sider, og lignende.

Enhver brug af internet søgning, udført på virksomheds IT udstyr, betragtes som virksomheds relateret, da det pågældende IT udstyrs IP adresse er unik. Dette betyder at virksomhed, hvis dette af virksomheden vurderes relevant, - kan vælge at gennemgå internet- browser og besøgte hjemmeside adresser. Medarbejder vil, hvis virksomheden gennemgår internet- browser, blive informeret herom.

Regler om brug af sociale medier i arbejdstiden:

Følgende regler gælder for anvendelse af sociale medier i arbejdstiden til privat formål:

- *Medarbejder kan i forbindelse med pauser (kaffe pause, frokost pause og lignende aftalte pauser) anvende sociale medier til private formål*
- *Medarbejder kan ikke anvende sociale medier i den pågældendes aftalte arbejdstid udenfor pauser*

Regler for hjemmearbejdspladser / it som medarbejder har med hjem.

Følgende regler gælder for IT udstyr, som medarbejder har adgang til hjemme.

- *Må familien bruge hjemme-pc en ?*
- *Må der installeres andre programmer end arbejdsrelaterede ?*
- *Hvordan skal pc opbevares i hjemmet (adgang og beskyttelse)*
- *Fortrolighed – i forhold til arbejdsrelaterede oplysninger, sikret så ikke andre kan få adgang ?*
- *Password og log in / log ud*
- *Brug af opkobling til fælles netværk (VPN eller lignende)*
- *Kontrol med at virus program og firewall er opdateret og at der køres fuld virus scan*
- *Trådløs internet – skal altid være forsynet med password og hvis der sendes / modtages personfølsomme oplysninger skal netværket ligeledes anvende kryptering.*

(Se informationer og vejledning fra http://di.dk/SiteCollectionDocuments/Shop/Itsikkerhedpaapchjemmearbejdspladsvejledning.pdf)

Overtrædelser:

Overtrædelse af virksomhedens IT sikkerhedspolitik og øvrige regler i dette dokument, vil medføre en skriftlig advarsel. I tilfælde af misbrug som er vurderet at være særligt skadeligt for virksomheden, kan der blive tale om bortvisning og opsigelse, eller ændring af arbejdsopgaver og beføjelser.

Advarsler som gives skriftligt, gemmes i virksomheden i op til 3 år.

Navn: Simon Groth_____ Dato: 01-11-2022_____

Underskrift af virksomheds ejer / direktør/ DATAANSVARLIG:

Ændringslog:

Dato	Vedrørende	Initialer
01.11.2022	Version 1.1	SHG