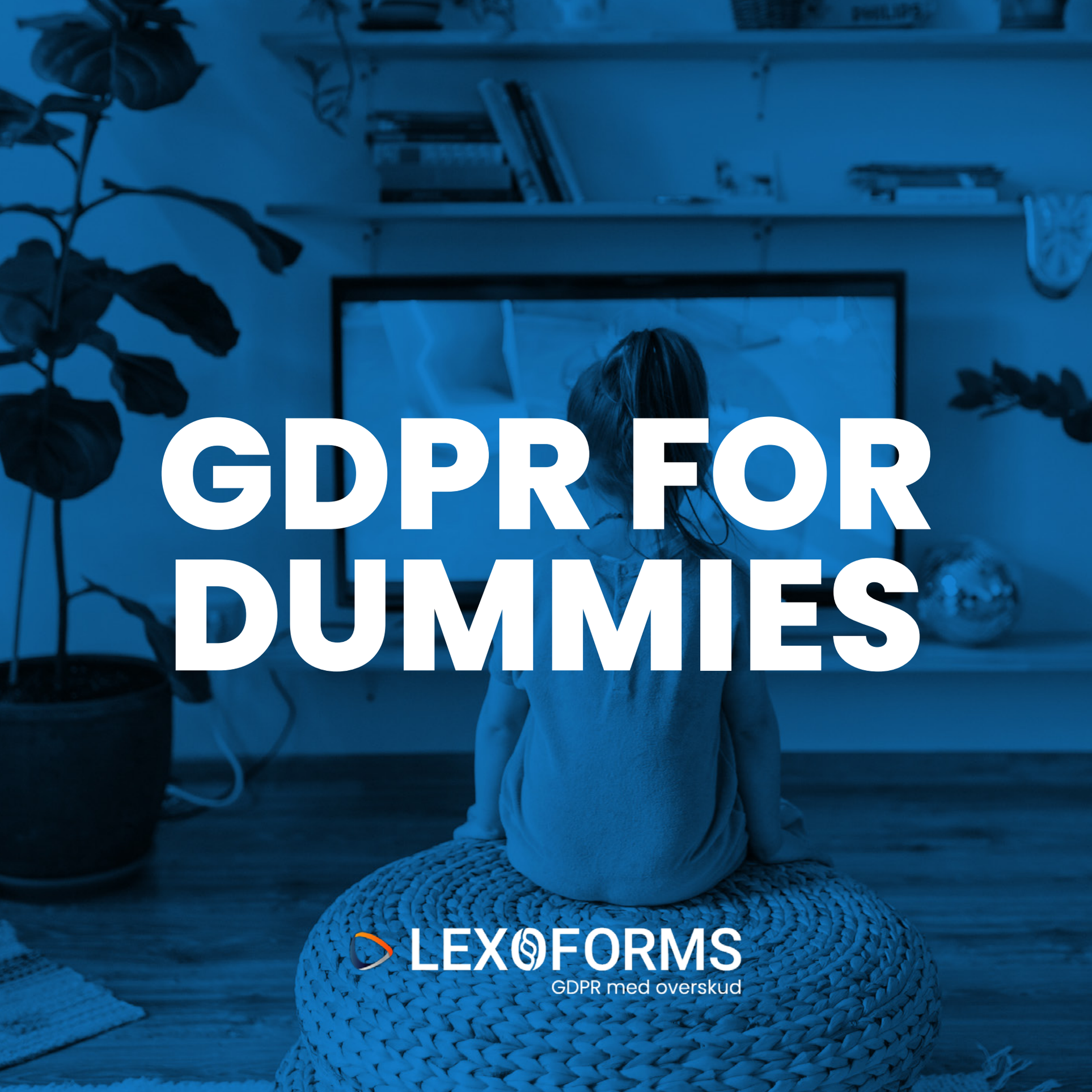

GDPR FOR
DUMMIES
LEXOFORMS
GDPR med overskud

Sådan får du styr på

Selvom flere tror, at GDPR er en uoverkommelig opgave, er det faktisk ikke så svært, som mange gør det til.

Med en oppefra-og-ned tilgang skal I ikke kortlægge samtlige processer "på gulvet", men kan i stedet nøjes med at fokusere på de overordnede hovedformål, så I kun registrerer de samme data én gang.

Så giver resten nemlig tit sig selv.

GDPR i bare 5 trin...

Det kræver vilje, struktur og lidt tid at komme i mål med GDPR-indsatsen. Eller rettere komme hen til Start.

For GDPR er ikke kun en kortlægning – det er en løbende opgave.

Til gengæld er gevinsten bedre overblik, øget effektivitet, højere sikkerhed og ikke mindst større ansvarlighed.

Grundlæggende er der fem trin, I skal have styr på...

1 2 3 4 5

1 Kortlæg data

I stedet for at beskrive alle mulige og umulige processer på alle mulige niveauer, er det langt smartere at tage udgangspunkt i de IT-systemer, I allerede bruger.

Dels ligger 90% af de relevante data her, dels giver en **oppefra-og-ned** tilgang langt hurtigere et godt overblik.

Det handler om at identificere hvilke personhenførbare oplysninger, I gemmer ***hvor*** og ***hvorfor***. Det handler også om, hvordan I håndterer dem. Både internt og eksternt.

Endelig skal I have en **slettepolitik** for de persondata, I ikke længere kan gemme med gyldig hjemmel. Inkl. klare kriterier for hvornår hvilke personoplysninger slettes.

2 Kortlæg aftaler

Alle virksomheder med et CVR-nummer er som udgangspunkt **dataansvarlige**. Desuden arbejder mange sammen med partnere, der får adgang til de personoplysninger, de opbevarer. Og det skal der være styr på.

Som dataansvarlig skal I have aftaler med alle jeres databehandlere – og hvis I også selv optræder som databehandler, skal I tilmed have styr på de **databehandleraftaler**, I selv har med jeres kunder.

Sidst men ikke mindst skal det være defineret og beskrevet, hvordan I fører **tilsyn og/eller kontrol** med jeres databehandlere. Som en tommelfingerregel er det den dataansvarlige, der fører tilsyn/kontrol med sine leverandører (databehandlere/underdatabehandlere).

3 Kortlæg risiko

Uanset hvad I gør, er der altid en risiko for, at noget går galt. Faktisk skyldes langt de fleste databrud menneskelige fejl som fx at sende en mail til en forkert modtager.

Det skal der være styr på!

Derfor er det vigtigt at afdække risikoen ved et sikkerhedsbrud inkl. mulig **konsekvens** for de registrerede, og hvor stor **sandsynligheden** er for et sikkerhedsbrud.

Teknisk og systemmæssigt skal alle it-systemer være så sikre som muligt. Fra it-struktur til kryptering, backup etc.

Organisatorisk skal alle relevante medarbejdere vide, hvad de skal gøre, hvorfor og ikke mindst hvordan.

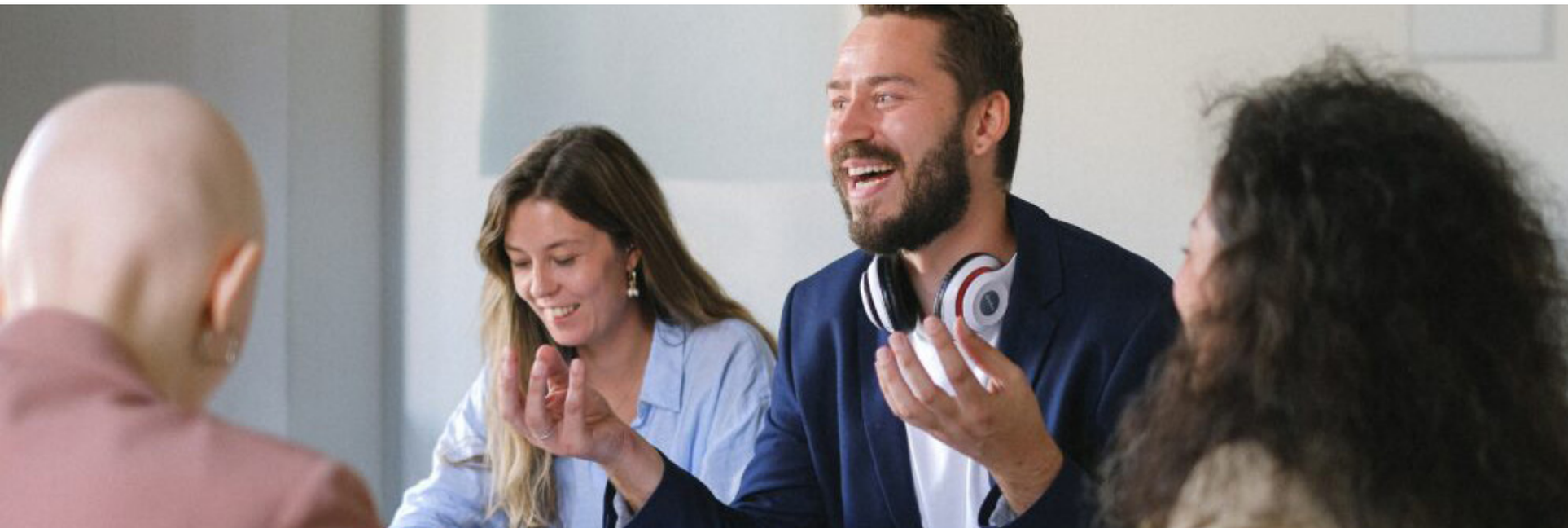
Fysisk skal bygninger, lokaler og udstyr kortlægges med fokus på at minimere risikoen for et sikkerhedsbrud.

4 Implementering

Når alle de basale ting som data, aftaler og risici er kortlagt, er det på tide at tage værktøjskassen under armen og få tingene indarbejdet i dagligdagen.

Internt skal alle medarbejdere vide, hvordan de skal håndtere hvilke data, uanset om de sidder i økonomi, HR, IT, indkøb, salg og marketing eller kundeservice.

Her er **medarbejderinstruksen** en stor hjælp til at sikre, at alle i hele organisationen ved, hvordan de skal forholde sig til persondata.



Data, håndtering og

Som dataansvarlig har I pligt til at **oplyse** alle registrerede om jeres håndtering af deres persondata samt deres rettigheder.

Hvilke personoplysninger opbevarer I, og...

· hvad skal de *bruges* til?

· hvad er *formål* og hjemmel?

· hvilke *interne brugere* har adgang til hvilke data?

· hvilke *eksterne brugere* har adgang til hvilke data?

Bruger I persondata til andet end det, en person som udgangspunkt har givet sin accept til, skal I sikre jer, at vedkommende aktivt giver sit **samtykke** til dette.

oplysningspligt

Endelig skal I **informere** om hvor længe, I opbevarer de pågældende personoplysninger, ligesom I skal informere om retten til indsigt, berigtigelse, begrænsning, udlevering, sletning og klage.

Det omfatter både de personoplysninger, I indsamler via jeres hjemmeside (fx formularer og cookies), men også dem, I får fra ansøgere, ansatte, kunder, leverandører og samarbejdspartnere.

Et sidste meget vigtigt punkt er sikkerheden, hvor I skal have en defineret **sikkerhedspolitik** samt **beredskabsplaner** for hvad I gør, hvis der opstår et databrud, eller hvis I får indsigelser eller anmodninger om indsigt fra fx nuværende eller tidligere kunder eller ansatte...

5 Drift

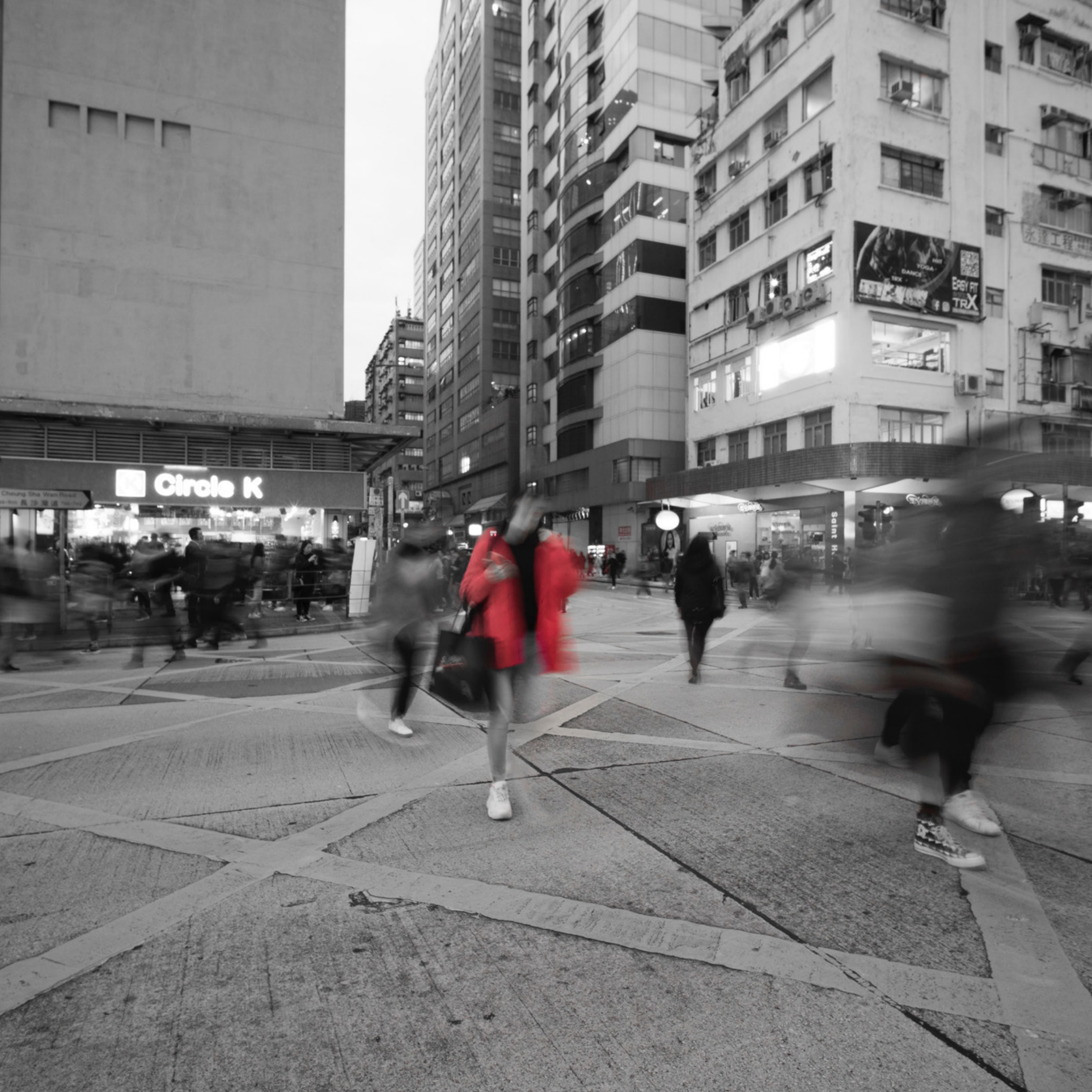
Det er først, når I har styr på data, databehandlere, risici, kommunikation og sikkerhed at det reelle arbejde med GDPR begynder.

I skal nemlig løbende sikre, at alt til enhver tid er **up-to-date** inkl. planlægning og gennemførsel af relevante tiltag – både manuelle og automatiske.

Det kan fx være ny software, ansøgere, nye kunder, opsagte medarbejdere, ændrede rutiner, nye bygninger, opdateringer, gennemgang af risikovurdering og personoplysninger, der skal slettes.

Alle disse kontroller skal **defineres** og **planlægges** – og ikke mindst **udføres**. For det hjælper ikke kun at beskrive hvilke kontroller, der skal laves og hvordan.

Det skal faktisk også gøres.


Circle K
YOGA
DANCE
TRX
TRX

+ Dokumentation

GDPR er ikke en sport, hvor man kommer i mål. Men når I først har været gennem alle de grundlæggende trin, er det meget lettere at holde jeres dokumentation **vedlige**.

For GDPR er en **løbende indsats**, hvor alle væsentlige ændringer i fx IT-systemer eller kundebase skal føres ajour, så alle data til enhver tid er opdaterede og kan dokumenteres på forlangende.

Det gælder både den generelle status samt hændelser som fx indsigtsanmodninger og sikkerhedsbrud.

= Intern fortegnelse

Den samlede kortlægning af data, databehandlere og risici samles i den interne fortegnelse, der på juridisk også kaldes en artikel 30-fortegnelse.

Den er **lovpligtig** og dokumenterer, hvordan I behandler de persondata, I har indsamlet. Den skal altid være 100% opdateret, og er på den måde et **dynamisk dokument**, der skal opdateres hver gang, I foretager en ændring.

Udover at skabe et internt overblik skal den interne fortegnelse også kunne **fremvises på forlangende**, hvis fx Datatilsynet kommer på besøg.

Derfor skal den kunne genereres på stedet – og det kræver et system, der kan **håndtere data i realtid**.

Den interne fortegnelse skal både kunne fremvises i rollen som dataansvarlig og databehandler.

Hændelser + it-brud

Sker der sikkerhedsbrud på persondata skal jeres håndtering dokumenteres – og er der risiko for de registrerede, skal hændelsen indberettes til Datatilsynet.

Men uanset om hændelsen skal indberettes til Datatilsynet eller ej, skal den **dokumenteres** med dato og tidspunkt, samt hvad der er sket – og hvorfor.

Det skal også beskrives hvilke personoplysninger, der er berørt, ligesom der skal laves en **risikovurdering** af, hvilke konsekvenser bruddet kan få for de berørte personer.

Det skal også fremgå, hvilke **afhjælpende foranstaltninger** der er truffet, og om Datatilsynet og/eller de berørte personer er **informeret** – eller hvorfor ikke.

Alle væsentlige beslutninger ifm. databruddet skal med andre ord dokumenteres i en log.

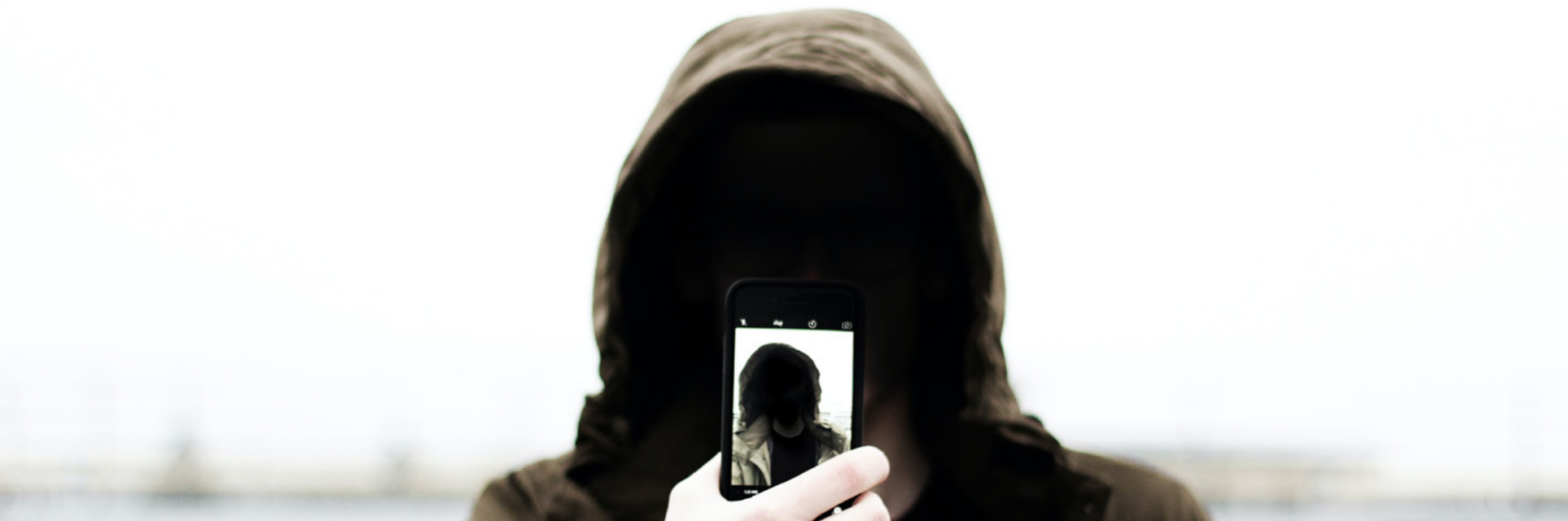
Indsigt + indsigelser

Med stadig flere registrerede persondata stiger også sandsynligheden for, at ansatte, kunder eller andre gerne vil vide, hvad I egentlig har liggende på dem.

Det skal der være en helt klar rutine for.

Derfor skal I have styr på, **hvor hvilke data ligger** (om alle registrerede), ligesom I skal have en **ansvarlig person**, der kan sikre korrekt berigtigelse, begrænsning, udlevering og sletning af data.

Og det hele skal **dokumenteres**...



GDPR handler om mennesker

Lexoforms ønsker at lette arbejdet med at dokumentere GDPR for små og mellemstore virksomheder på en korrekt, brugervenlig, uvildig og enkel måde.

GDPR handler nemlig om at passe på hinanden og udvise respekt de data, andre betror os.

Med vores løsning skal du kun registrere de samme data én gang. Det gør hele opgaven lidt lettere...

LEXOFORMS
lexoforms.com