Rie Aleksandra Walle
Grumpy DPO

Følg meg på:
linkedin.com/in/riealeksandra

🎙️ Hør på **Grumpy GDPR podcast:**
https://www.noties.consulting/grumpy/

💌 Abonner på **The Curated DPO newsletter:**
https://www.noties.consulting/eletter/

📧 **Ta kontakt for foredrag, kurs, workshop for din kommune(r): rie@bedrebedrift.no**

DEATH BY RISK ASSESSMENTS

Rie Aleksandra Walle

Grumpy DPO, NoTies Consulting

Snakkepunkter

Puste liv i risikoprosessen

Risikoworkshop

Lærdommer og tips

“risikovurderinger”

Hvorfor gidde?

Vær forberedt

4. Krav om redegjørelse

Vi ber kommunen sende oss følgende:

4.1 Kommunens behandlingsprotokoll, jf. artikkel 30

4.2 Oversikt over kommunens organisering av ansvarsforhold knyttet til etterlevelse av personvernregelverket, jf. artikkel 5 nr. 2

4.3 En kort beskrivelse av kommunens overordnede styringssystem (internkontroll) for etterlevelse av personvernregelverket, herunder hvilke verktøy som eventuelt brukes

4.4 Styrende retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser, jf. artikkel 32

4.5 Kommunens eventuelle overordnede sikkerhetsstrategi

4.6 Oversikt over eventuelle IKT-samarbeid med andre kommuner

4.7 Styrende retningslinjer for autentiseringsløsninger i kommunen

4.8 Styrende retingslinjer for sikkerhetskopiering og gjenoppretting av systemer, jf. artikkel 32.1.c)

4.9 Styrende retningslinjer/prosedyrer for sikkerhetsrevisjoner, jf. artikkel 32.1.d)

4.10 Lenke til kommunens personvernerklæring

4.11 Informasjon om kommunens personvernombud, herunder:

- Navn, telefonnummer og e-postadresse til personvernombudet i kommunen
- Kort beskrivelse av organiseringen av personvernombudsfunksjonen; herunder hvor stor del av full stilling vedkommende skal kunne bruke på utevelsen av rollen
- Lenke til kommunens nettside som inneholder informasjon om personvernombudet

Helsingørgate

Hvordan gjøre tilsynskontrollen verst mulig for deg selv

…eller ev. lykkes med leverandøroppfølging

“på sin egen tue”

“på sin egen tue”

“på sin egen tue”

“på sin egen tue”

“på sin egen tue”

“på sin egen tue”

“på sin egen tue”

Hvorfor gidde?

(risikovurderinger)

Oversikt
Innsikt
(bedre) Kontroll

årsak 1:

Jeg gjør det for formelt og vanskelig å forstå

Tradisjonell ROS

GDPR-perspektiv

årsak 1:

Jeg gjør det for formelt og vanskelig å forstå

MITIGERENDE TILTAK

Rie Aleksandra Walle (She/Her) • You
Grumpy GDPR 🪨 | Speaker & Lecturer | Transitional/Emergency D...
2w • Edited •

😍 Is this my dear carpenter I'm seeing **Datatilsynet**?? OK, I might not be able to take credit for this but I'm ecstatic anyway to see that you've not only provided GDPR guidance for small businesses, but a whole UNIVERSE. 💫

Which starts with 7 key steps to GDPR compliance:
1. Get an overview
2. Ask yourself "Why?"
3. Remember to delete
4. Inform when you process personal data
5. Ensure you have robust policies and procedures
6. Remember security
7. You're also responsible when you *share* personal data

Great tips right there for both small and large businesses and organizations! Creation of Datatilsynet, **Dansk Erhverv**, **DI - Dansk Industri** and **SMVdanmark**.

I also applaud Datatilsynet for using "jævnt dansk" 🇩🇰 in their descriptions, which we'd call "folkelig språk" here 🇳🇴, that is: written in a way that most people would understand. Cannot emphasize how important this is.

DATATILSYNET

Nyt vejlednings-univers

GDPR for små virksomheder

Dato: 04-05-2023

Nyhed

Datatilsynet har lavet et nyt vejledningsunivers om GDPR til mindre virksomheder. Vejledningsuniverset er udviklet med fokus på overskuelighed og konkrete eksempler, og så er det skrevet på jævnt dansk.

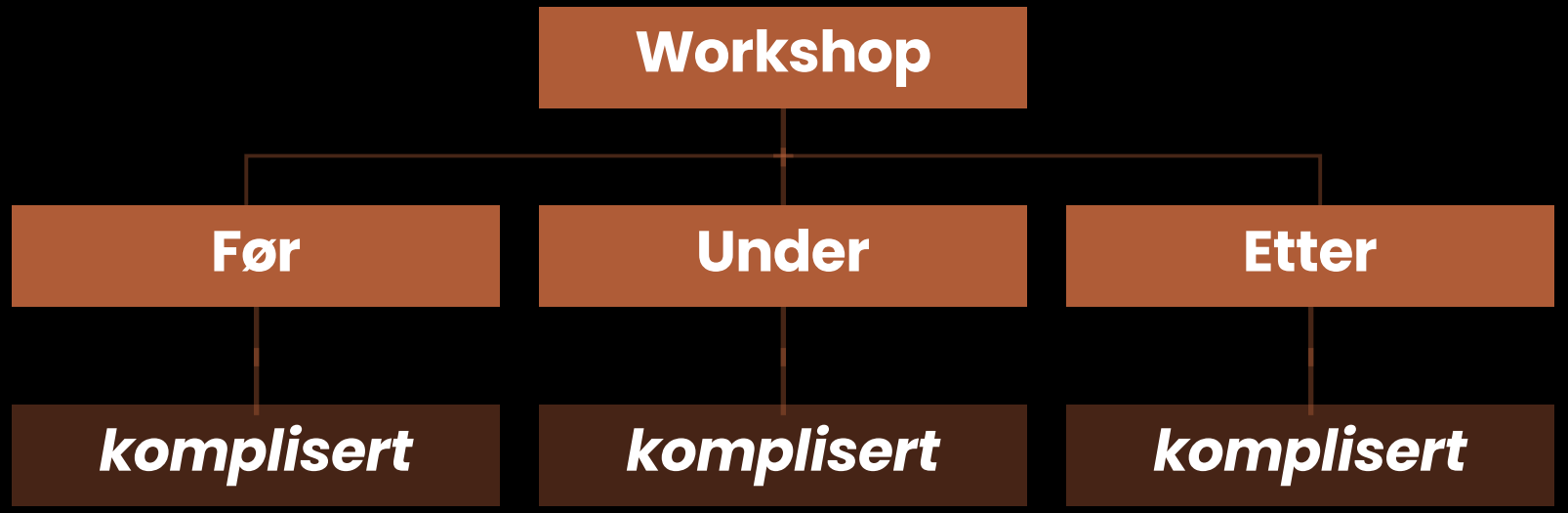
I dag lancerer Datatilsynet et nyt vejledningsunivers særligt målrettet små virksomheder.

"Vi ved, at det for mange små virksomheder kan virke uoverkommeligt at få styr på GDPR. Reglerne gælder for både store og små virksomheder, men ofte er opgaven noget mere overkommelig for de mindre virksomheder, hvis de får den rette hjælp," siger Cristina Angela Gulisano, direktør i Datatilsynet, og fortsætter:

"Vi vil i Datatilsynet derfor gerne gøre GDPR nemmere at gå til – især for de mindre virksomheder, der ikke har medarbejdere med juridiske forudsætninger til at omsætte de fleksible men samtidig til tider

årsak 2:

Jeg drukner folk i metodikk, regneark, systemer...



årsak 2:

Jeg drukner folk i metodikk, regneark, systemer...

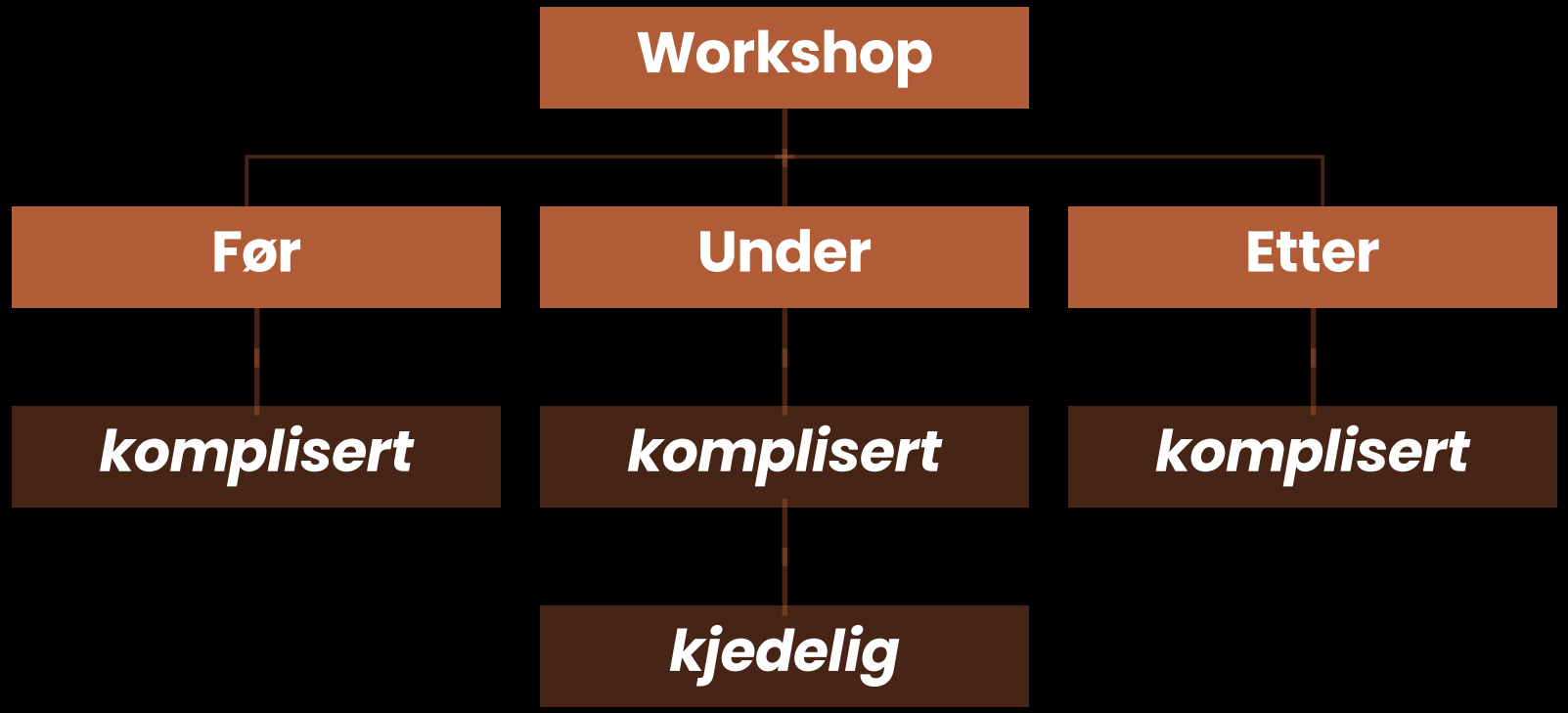
MITIGERENDE TILTAK

årsak 3:

Jeg gjør det for kjedelig

Velkommen til risikovurderingsworkshop!

I personvernforordningen (GDPR) skal vi gjennomføre risikovurderinger knyttet til behandlingen vår av personopplysninger. I en slik prosess skal vi identifisere og håndtere potensielle risikoer for personvernet til de vi behandler personopplysninger til. Målet er å sikre at personopplysninger behandles på en forsvarlig måte og i samsvar med gjeldende personvernlover og -forskrifter (inkludert personvernforordningen). For å gjennomføre en risikovurdering i praksis, følger man vanligvis noen trinn: 1. Identifisering av personopplysninger: Start med å kartlegge hvilke typer personopplysninger som behandles i organisasjonen. Dette kan inkludere informasjon som navn, adresse, fødselsdato, e-postadresse, men også metadata, registreringsnummer til kjøretøy, informasjonskapsler på en nettside og mer som umiddelbart kanskje ikke fremstår som personopplysninger. 2. Identifisering av risikoer: Identifiser potensielle trusler eller risikoer som kan påvirke personvernet. Dette kan inkludere hacking, datatap, uautorisert tilgang eller feilaktig bruk av personopplysninger. 3. Vurdering av sannsynlighet og konsekvens: Vurder hvor sannsynlig det er at risikoene vil materialisere seg, samt konsekvensene av en eventuell personvernskade. Dette kan gjøres ved å vurdere tidligere hendelser, bransjestandarder og potensielle skadeomfang. 4. Identifisering av kontroller: Identifiser hvilke kontroller eller tiltak som allerede er på plass for å redusere risikoene. Dette kan være tekniske sikkerhetssystemer, retningslinjer for ansatte, personvernavtaler eller andre tiltak for å beskytte personopplysninger. 5. Evaluering av risikonivå: Vurder risikonivået for hver identifiserte risiko ved å kombinere sannsynlighet og konsekvens. Dette kan gjøres ved hjelp av en risikomatrise eller en annen metode for å klassifisere risikoer i høy, middels eller lav kategori. 6. Utvikling av tiltak: Utvikle tiltak for å håndtere de identifiserte risikoene. Dette kan inkludere å implementere bedre sikkerhetsprotokoller, styrke passordpolitikken, opplæring av ansatte eller revisjon av eksisterende personvernregler. 7. Gjennomføring og oppfølging: Implementer de identifiserte tiltakene og følg opp for å sikre at de fungerer som tiltenkt. Dette kan inkludere testing av systemer, opplæring av ansatte og jevnlige revisjoner for å opprettholde et tilstrekkelig beskyttelsesnivå. En grundig risikovurdering knyttet til personvern er en kontinuerlig prosess som bør gjentas regelmessig, spesielt ved endringer i drift, teknologi eller lover og forskrifter som påvirker person. Dette kan inkludere informasjon som navn, adresse, fødselsdato, e-postadresse, men også metadata, registreringsnummer til kjøretøy, informasjonskapsler på en nettside og mer som umiddelbart kanskje ikke fremstår som personopplysninger. 2. Identifisering av risikoer: Identifiser potensielle trusler eller risikoer som kan påvirke personvernet. Dette kan inkludere hacking, datatap, uautorisert tilgang eller feilaktig bruk av personopplysninger. 3. Vurdering av sannsynlighet og konsekvens: Vurder hvor sannsynlig det er at risikoene vil materialisere seg, samt konsekvensene av en eventuell personvernskade. Dette kan gjøres ved å vurdere tidligere hendelser, bransjestandarder og potensielle skadeomfang. 4. Identifisering av kontroller: Identifiser hvilke kontroller eller tiltak som allerede er på plass for å redusere risikoene.

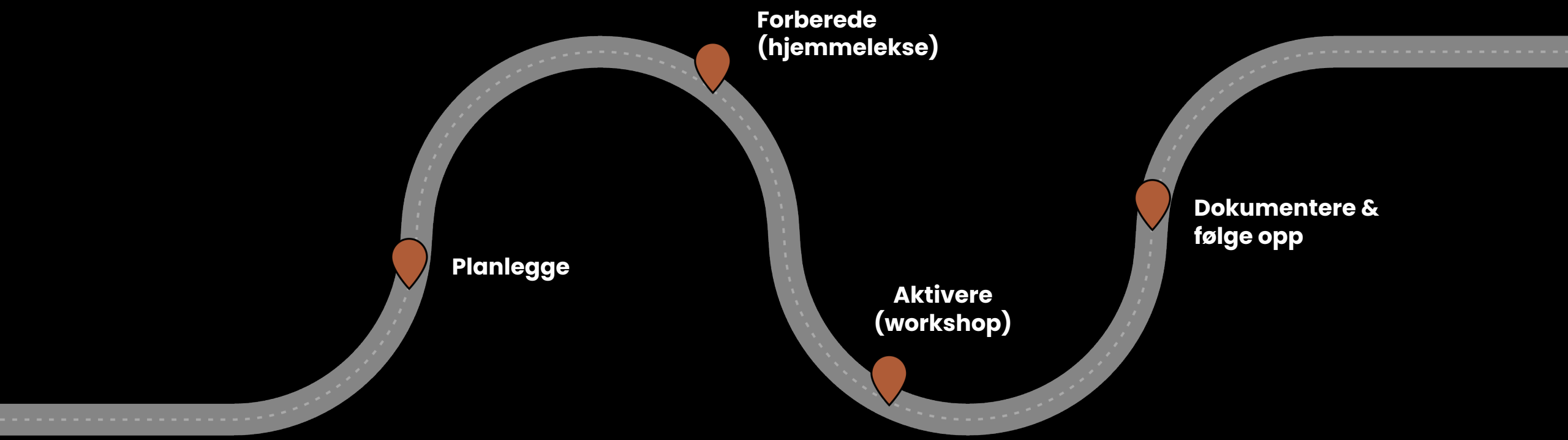


årsak 3:

Jeg gjør det for kjedelig

MITIGERENDE TILTAK

Risikoworkshop

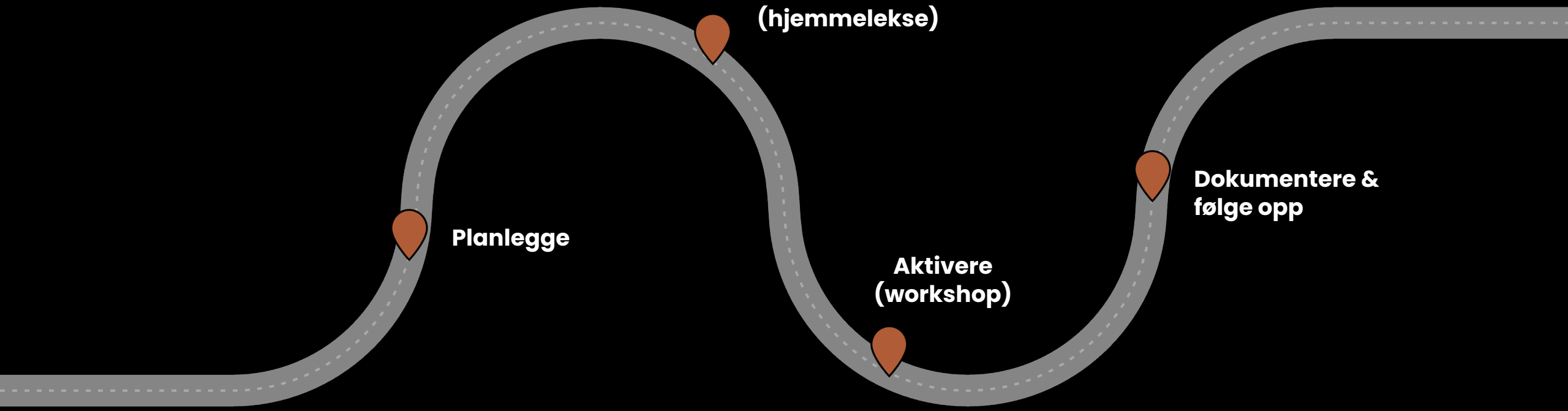


For formelt, vanskelig, komplisert, kjedelig og **tidkrevende**

For formelt, vanskelig, komplisert, kjedelig, tidkrevende **hypotetisk, teoretisk**

Arbeidet/tiltak følges ikke opp og blir ikke gjort

Risikoworkshop



- ~~**Formelt, komplekst, kjedelig**~~
- **Lettbent, forståelig, engasjerende, gøy!**
- **Solid prosess**
  - *Arbeidsgruppe, hjemmelekse, nøkkelroller, fokus: folk*
- **Dokumentér, dokumentér, dokumentér**
  - *Med datoer!*
- **Følg opp, følg opp, følg opp**
- **Gå ned fra tua di og lag fest på åsen!**
- **OG HA DET GØY!**