Solfi

Hva er egentlig...

GDPR?

Halvannen dusin lettleste slides som svarer på spørsmål du har forsøkt å unngå siden 2018.

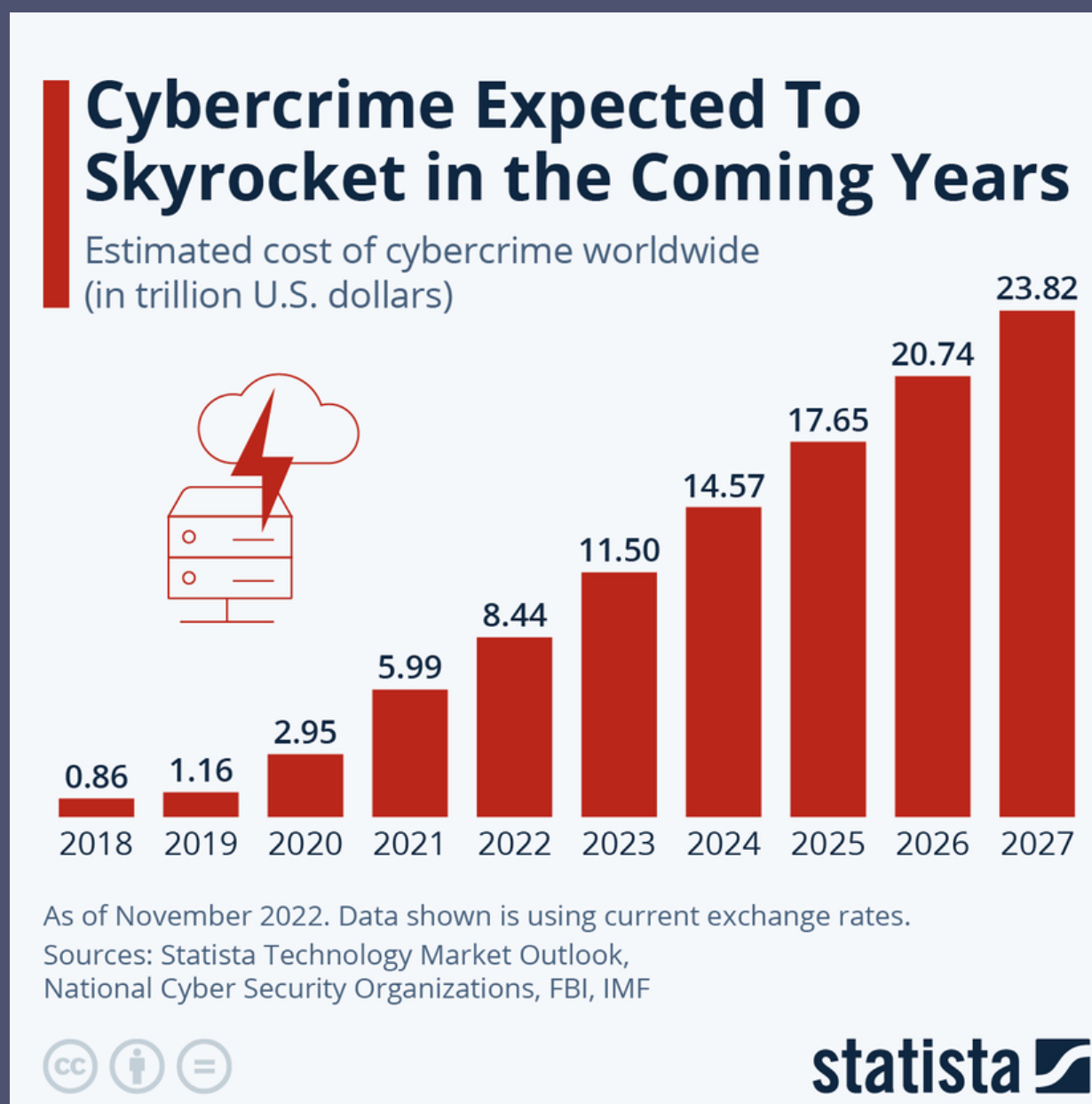
John Arthur Berg
Teknolog og rådgiver

Solfi

Men er det så viktig?

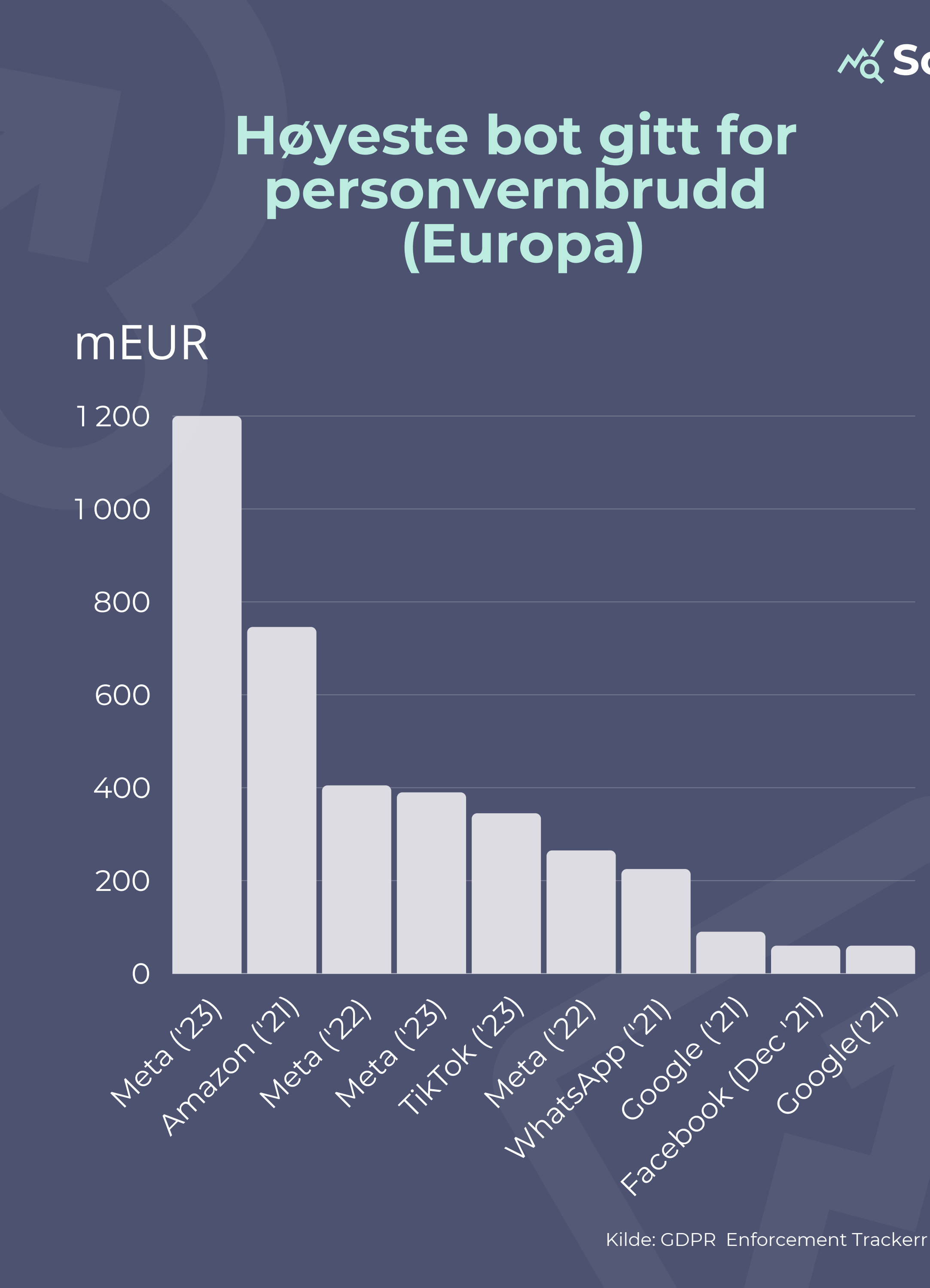
“Fight or flight” refleksen slår ofte inn hos ledere og utviklere når GDPR kommer opp som et tema. Men konsekvensene av brudd på personvernet kan være store.

Enorme kostnader med sikkerhetsbrudd og identitetstyveri



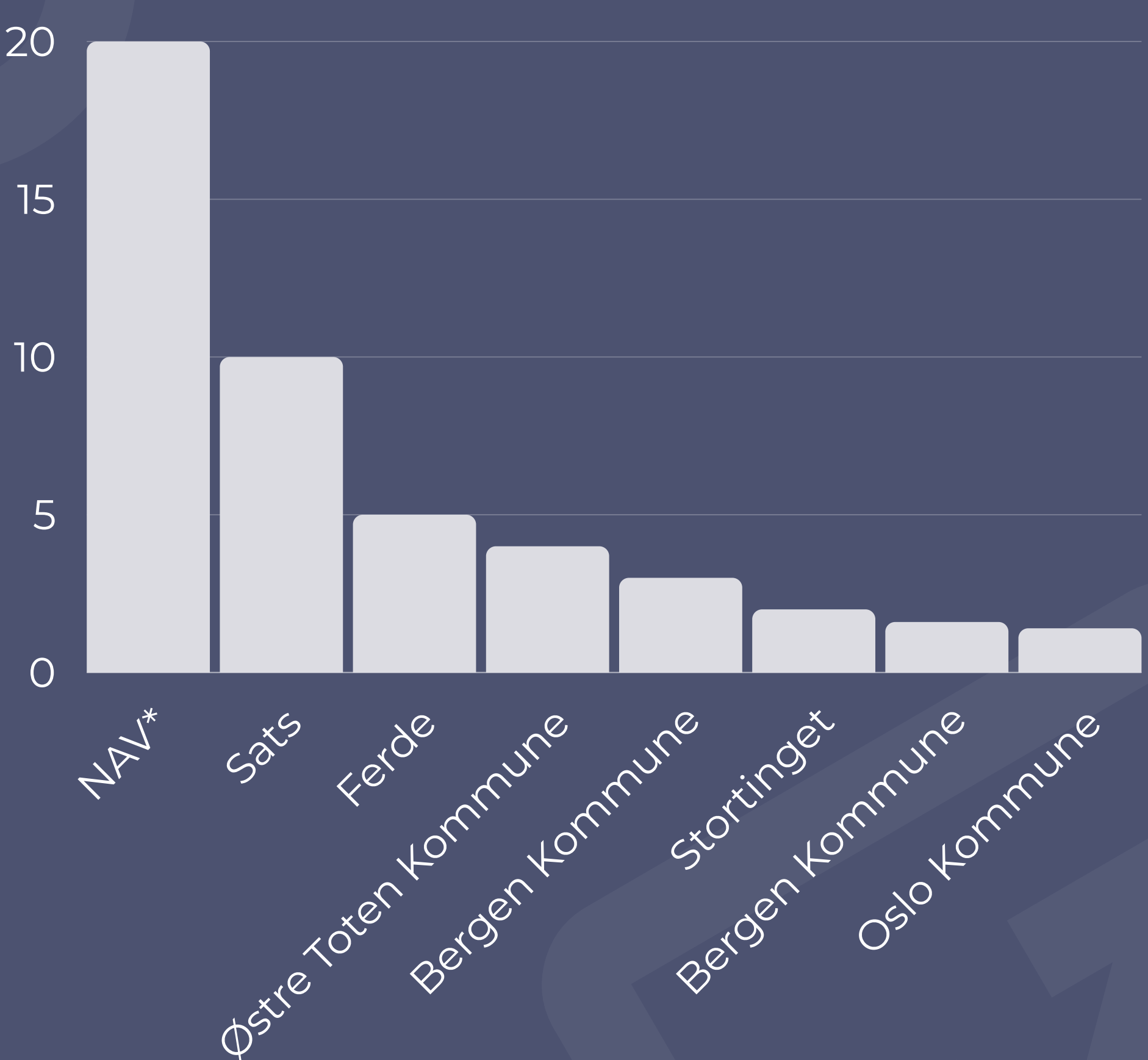
For de fleste typer virksomheter så er GDPR den mest relevante reguleringen knyttet til sikkerhet, og virksomheter kan bøtelegges for sikkerhetsmangler.

Høyeste bot gitt for personvernbrudd (Europa)



Kilde: GDPR Enforcement Trackerr

Høyeste bot gitt for personvernbrudd (norske virksomheter)



(* Ikke endelig vedtak)

Kilde: GDPR Enforcement Tracker og datatilsynet.no

Solfi

Men hva er egentlig persondata?

All informasjon som **direkte** eller **indirekte** kan identifisere en fysisk person.

Men ikke IP-adresse!?

Jo!!

Men ikke intern brukerID?!

Jo!!

Men ikke GPS koordinater?!

Jo!!

Men hva er egentlig persondata?

Eksempel:

- Navn
- Identifikasjonsnummer
- Lokasjonsdata
- Nettidentifikatorer

Definisjonen av persondata i GDPR er svært gjennomgripende. “Indirekte identifisere” betyr f.eks. at en IP addresse eller et GPS-spor er persondata. Mange typer data vi tenker på som “anonyme” er persondata under GDPR.

Solfi

Hvilke persondata kan jeg samle inn?

GDPR handler ikke om “hva”, men om **hvorfor** og **hvordan**.

Så lenge du behandler personopplysninger på en lovlig, rettferdig og åpen måte så kan det meste av persondata benyttes.

Unntaket er for det som er definert som “særlige kategorier av persondata”. Det gjelder f.eks. helseopplysninger, DNA, biometri, legning og etnisk opprinnelse. Det er forbudt å behandle slike opplysninger, unntatt til enkelte formål.

Solfi

“Behandling”?

Jeg er utvikler, hva i all verden betyr behandling?!

Alt du kan gjøre med data! Samle inn, slette, organisere, sammenstille, endre, vise, tilpasse, utlevere.

Ah. EDB. Elektronisk databehandling.

Dropp “E”-en. GDPR kan også gjelde for papirbasert behandling*.

(* I strukturert form)

Solfi

Hvordan behandler jeg persondata lovlig?

1. Ha et klart definert **formål** med behandlingen.
2. Behandlingen må **begrenses** (i omfang og tid) til formålet.
3. Du må ha et **lovlig grunnlag** for behandlingen (mer om det senere).
4. Du må være åpen om behandlingen (**transparent**) og respektere **rettighetene** til de registrerte.
5. Du må gjennomføre egnede **tekniske og organisatoriske tiltak** for å sikre behandlingen inkl. rutiner for varsling ved personvernsbrudd.
6. Du må inngå avtaler med tredjeparter som bistår i behandlingen (**databehandleravtaler**).

Solfi

Formål

Start med å definere formålet for behandlingen av persondata, det danner grunnlaget for etterlevelse av de fleste plikter under GDPR. Formålet skal være spesifikt!

Vi samler inn data for bruk i fremtidige tjenester som vi enda ikke har definert, i tilfelle vi behøver de.

Vi behandler dine persondata for å kunne sende varer du bestiller hos oss.

Solfi

Formål og begrensning

Personopplysningene må slettes når de ikke lenger tjener formålet.

Omfanget av personopplysninger må minimeres til kun det som er nødvendig for å tjene formålet.

Personopplysningene skal ikke brukes til andre formål eller utleveres til tredje parter.

Solfi

Behandlingens lovlighet

Behandlingen må baseres på (minst) ett av disse grunnlagene:

- **Et samtykke**
- **En avtale**
- **En rettslig forpliktelse**
- **Beskyttelse av personens interesser**
- **Offentlig oppgave eller i allmenhetens interesse.**
- **“Berettiget interesse”**

En vanlig misforståelse er at alt må ha samtykke. Men samtykke er ofte et dårlig grunnlag for behandlingens lovlighet.

Solfi

De registrertes rettigheter

Når persondataene behandles, har den registrerte lovbestemte rettigheter:

1. **Åpenhet om behandlingen**
2. **Informasjon og innsyn**
3. **Retting og sletting**
4. **Begrensning**
5. **Protestere mot behandling**
6. **Motsette seg automatiserte avgjørelser**

Disse rettighetene har begrensninger, de gjelder ikke alltid men avhenger av type behandling/lovgrunnlag.

Solfi

Sikkerhet

Teknisk sikkerhet som står i stil til omfang av person data som skal beskyttes, og konsekvenser hvis data kommer på avveie.

Internkontroll, gode prosedyrer, opplæring, dokumentasjon.

Rutiner for å varsle myndigheter og brukere hvis det skjer et alvorlig personvernsbrudd.

Solfi kan GDPR!

Vi skreddersyr opplæring for din virksomhet. Vi bistår også gjerne med workshops og hjelper til med implementering og internrevisjon.

Available in English

John Arthur Berg
+47 930 53 088
john.arthur.berg@solfi.no

Solfi

Vi hjelper vekstbedrifter å skalere