

# GDPR – SJEKKLISTE

## ORGANISERING AV ANSATTE

- Identifiser hvilke ansatte i din bedrift som har tilgang på personopplysninger og må være oppdaterte på GDPR.
- Oppnev et personvernombud om det er mange ansatte eller om dere behandler store mengder sensitive personopplysninger.
- Hvis bedriften har ansatte/kontorer utenfor EU, påse at relevante opplysninger og føringer når ut til dem.

## INTERNE SYSTEMER

- Vurder om din bedrift bør opprette et risikoregister.
- Kontroller at bedriftens prosedyrer er i samsvar med GDPR.
- Kontroller at prosedyrene ivaretar rettighetene individer har under GDPR.
- Vurder om dere trenger å samle alle ansatte for å informere om endringene i regelverket.
- Om nødvendig, påse at dere har iverksatt pålagte GDPR-tiltak for å innhente data om barn/ungdom, og sensitive personopplysninger.
- Påse at dere har rutiner for internkontroll og er i stand til å avdekke et datainnbrudd, og dermed iverksette tiltak og varsling i henhold til kravene under GDPR og datatilsynet.
- Foreta regelmessige sikkerhetskontroller av systemene, og påse at dataen dere lagrer er sikret på en forsvarlig måte.

## DATABEHANDLING

- Dokumentér hva slags personopplysninger bedriften samler inn, hvor dataen kommer fra, hvem bedriften deler data med, og hvordan data skal benyttes av både dere og 3. part.
- Påse at bedriften har rutiner for innsyn, retting og sletting av kundedata når kunder ber om det.
- Påse at bedriften enkelt kan skaffe kunder en kopi av all data bedriften lagrer om dem.
- Planlegg i forkant hvordan bedriften skal ta hånd om GDPR-forespørsler i tråd med fristene fra personvernforordningen og Datatilsynet.
- Gjennomgå hvilke data bedriften tar inn, og identifiser det rettslige grunnlaget for denne type data (inkludert cookies og personvernerklæring), og dokumenter hvordan og hva dere kom frem til.
- Gjennomgå metodene for å innhente samtykke, slik at de er i tråd med GDPR. Bedriften må vise at gyldig samtykke ble innhentet og gitt i tråd med regelverket og skriftlig. For eksempel ved utsending av nyhetsbrev.
- Finn ut og dokumenter hvem alle databehandlere og behandlingsansvarlige er, hvor dere må ha databehandleravtaler, og planlegg relevant trening/kursing for de ansatte.

## INTERESSETER

- Kontakt kunder for å informere, gå gjennom, oppdatere dem på bedriftens og deres GDPR ansvar, og om endringene bedriften har foretatt eller vil foreta under GDPR. Husk å dokumentere dette.
- Informer alle involverte, 3. parter, eiere og investorer om dataen dere innhenter, deler og behandler, samt om frister og risikoer rundt GDPR.
- Rutine for varsling av avvik (brudd på konfidensialitet/integritet/tilgjengelighet) innen 72 timer.



**HJELP!** Synes du listen inneholder mye som må løses og at det er vanskelig å forstå alle de juridiske formuleringene i lovkravene? Vi er klar over at GDPR er et omfattende og komplisert regelverk som krever nye rutiner og mye dokumentasjon som det er tidkrevende å sette seg inn i. Derfor har vi utviklet et GDPR-verktøy som på en enkel måte hjelper dere å kartlegge firmaets GDPR-situasjon, samt dokumentere og løse de fleste av punktene på sjekklisten. Verktøyet produserer en tiltaksliste som beskriver hvilke oppgaver som må løses, samt rapport som grunnlag for internkontroll. Se [www.datatilsynet.no](http://www.datatilsynet.no) for informasjon om virksomhetenes plikter.