

FOR HR:

GDPR-sjekkliste



 Sympa

Denne sjekklisten vil hjelpe deg med å danne en oversikt over hvilke systemer du lagrer hvilke data i, samt finne ut om din organisasjons retningslinjer for datalagring er i samsvar med EU-lovgivningen om datasikkerhet.

Dokumentet inneholder også nyttige spørsmål som kan hjelpe deg å finne ut om partnerne dine overholder lovgivningen.

Personvernrettigheter

Spørsmål	Hvorfor er det viktig å stille dette spørsmålet?	Ja	Nei	Vet ikke	
Er det lett for deres medarbeidere å be om og motta alle opplysninger du har lagret om dem?	Medarbeiderne har rett til å få innsikt i de personopplysningene dere har registrert om dem, og hvordan dere bruker disse.				
Er det lett for deres medarbeidere å korrigere eller oppdatere feilaktig eller ukomplett informasjon?	Medarbeiderne har rett til å korrigere feilaktige data.				
Er det lett for deres medarbeidere å be om at deres personlige opplysninger blir slettet?	Medarbeiderne har rett til å be om å slette alle personopplysninger dere har registrert om dem. Du må kunne oppfylle denne forespørselen i løpet av en måned.				
Er det lett for deres medarbeidere å be dere om å stoppe all behandling av deres personopplysninger?	Medarbeiderne kan be om at all håndtering av deres data blir stoppet eller begrenset på midlertidig grunnlag hvis visse vilkår er oppfylt.				
Er det lett for deres medarbeidere å motta en kopi av de personopplysningene dere har registrert, i et format som enkelt kan bli overført til en annen bedrift?	GDPR krever at dere må kunne lagre en fil med de relevante personopplysningene i et vanlig format som de fleste kan lese, og senere sende disse til medarbeideren eller en angitt tredjepart. Dette representerer grunnprinsippet i GDPR, om at enkeltpersoner eier sine egne data, ikke bedriftene.				
Er det lett for deres medarbeidere å protestere på at dere behandler personopplysningene deres?	Hvis du bruker automatiserte prosesser for å hjelpe til med å ta beslutninger som har en betydelig innvirkning på medarbeiderne, må du definere en prosedyre som sikrer at du beskytter medarbeidernes rettigheter. Du må også gjøre det enkelt for medarbeiderne å be om en personlig vurdering, påvirke beslutninger og utfordre beslutninger du allerede har tatt.				

Personvernrettigheter

Spørsmål	Hvorfor er det viktig å stille dette spørsmålet?	Ja	Nei	Vet ikke
ikkeHvis dere tar avgjørelser om deres medarbeidere basert på en automatisert prosess, har dere en prosedyre på plass for å beskytte deres rettigheter?	Hvis du bruker automatiserte prosesser for å hjelpe til med å ta beslutninger som har en betydelig innvirkning på medarbeiderne, må du definere en prosedyre som sikrer at du beskytter medarbeidernes rettigheter. Du må også gjøre det enkelt for medarbeiderne å be om en personlig vurdering, påvirke beslutninger og utfordre beslutninger du allerede har tatt.			

Datasikkerhet

Spørsmål	Hvorfor er det viktig å stille dette spørsmålet?	Ja	Nei	Vet ikke
Er dataene dine krypterte, pseudonymiserte eller anonymiserte der det er mulig?	GDPR krever at organisasjoner benytter seg av kryptering eller pseudonymisering på alle områder det er mulig.			
Har dere iverksatt tiltak som sikrer påfølgende kontroll og verifisering av identiteten til personer som har registrert, endret eller overført personopplysninger?	GDPR krever at personopplysninger blir behandlet på en måte som sikrer den tilstrekkelige konfidensialiteten til dataene. Det inkluderer alle tiltak som forhindrer uautorisert tilgang til, eller bruk av personopplysninger, og utstyret som benyttes til behandlingen.			
Har dere interne tiltak på plass for å forhindre uautorisert tilgang til personopplysninger?	GDPR krever at personopplysninger blir behandlet på en måte som sikrer den tilstrekkelige konfidensialiteten til dataene. Det inkluderer alle tiltak som forhindrer uautorisert tilgang til, eller bruk av personopplysninger, og utstyret som benyttes til behandlingen.			

Datasikkerhet

Spørsmål	Hvorfor er det viktig å stille dette spørsmålet?	Ja	Nei	Vet ikke
Har dere iverksatt tiltak som sikrer en kontinuerlig konfidensialitet, integritet, tilgjengelighet og motstandsdyktighet på alle systemer og tjenester som benyttes til behandling av personopplysninger?	De systemene og programmene dere benytter må være forberedte på databrudd. GDPR krever at dere har muligheten til å kunne gjenopprette tilgjengeligheten til personopplysninger i tide hvis det skulle oppstå en fysisk eller teknisk hendelse.			
Har dere etablert en prosess for regelmessig testing, vurdering og evaluering av effektiviteten til tekniske og organisatoriske tiltak for å sikre at behandlingen foregår på en sikker måte?	GDPR krever at disse tekniske og organisatoriske tiltakene skal revideres jevnlig, og oppdateres om nødvendig. Hvis dere bruker en ekstern behandler, er det opp til dem å sørge for at dette kravet blir overholdt.			
Har dere etablert en prosess for å varsle myndighetene og de berørte hvis dere blir utsatt for et databrudd?	Hvis det har oppstått et databrudd og personopplysninger har blitt lekket, er det et krav om at dere må varsle ansvarlig myndighet innen 72 timer. Dere må også raskt informere om databruddet til de berørte, med mindre det er fare for at bruddet utsetter dem for risiko. Hvis dere bruker en ekstern behandler, er det opp til dem å sørge for at dette kravet blir overholdt.			

Ansvarlighet og styring

Spørsmål	Hvorfor er det viktig å stille dette spørsmålet?	Ja	Nei	Vet ikke	
Har dere inngått en databeskyttelsesavtale mellom deres organisasjon og tredjeparter som behandler HR-relaterte personopplysninger for dere?	GDPR krever at all form for behandling av tredjeparter må være underlagt en kontrakt. Lovgivningen har en detaljert oversikt over de punktene som partene må være enige om.				
Har dere oppnevnt en representant i en av medlemslandene til EU hvis organisasjonen din holder til utenfor EU?	Hvis dere behandler data for personer som bor i et bestemt medlemsland kan det hende at dere må oppnevne en representant i dette landet som kan kommunisere på deres vegne med landets datatilsyn.				
Har dere utnevnt et personvernombud?	Det er tre årsaker til at organisasjoner må utnevne et personvernombud, men det er ingen dårlig ide å utnevne et selv om reglene ikke gjelder dere. Personvernombudet må være en ekspert på databeskyttelse.				

Lovgrunnlag og åpenhet

Spørsmål	Hvorfor er det viktig å stille dette spørsmålet?	Ja	Nei	Vet ikke	
Har dere gjennomført en informasjonsrevisjon for å registrere hvilken form for informasjon dere behandler, og hvem det er som har tilgang til informasjonen?	Organisasjoner som har minst 250 ansatte eller utfører en databehandling med høyere risiko, er pålagt å holde en oppdatert og detaljert liste over alle behandlingsaktiviteter , samt være forberedt på å vise denne listen til ansvarlig myndighet på forespørsel. Organisasjoner med færre enn 250 ansatte bør også gjennomføre en vurdering siden det vil gjøre det lettere å overholde de øvrige kravene i GDPR.				
Har dere utført en konsekvensanalyse relatert til databeskyttelse?	GDPR krever at en konsekvensanalyse utføres når behandlingsaktiviteten utgjør en stor risiko for rettighetene og friheten til berørte personer. Hvis dere bruker en ekstern behandler, er det opp til dem å sørge for at dette kravet blir overholdt.				
Har dere gitt en tydelig informasjon om databehandlingen og det lovlige grunnlaget i bedriftens personvernregler?	Dere må informere om at dere samler inn personopplysninger og hvorfor dere gjør det. Dere må forklare hvordan personopplysningene blir behandlet, hvem som har tilgang til dem og hvordan dere sikrer dem. Denne informasjonen må være inkludert i bedriftens personvernregler og overleveres til eierne av personopplysningene når dere samler inn deres data.				

Om oss

Sympa leverer det beste helhetlige HR-systemet som sømløst håndterer hele arbeidsforholdet til medarbeiderne. Den er multi-geo, enkel å bruke og fleksibel. Dessuten lar Sympas omfattende økosystem deg integrere alle dine andre HR-verktøy for å sikre smidig datadeling og arbeidsflytøverganger mellom systemer. Plattformen vår er utstyrt med unike samarbeidsfunksjoner som gjør HR og bedriftsledere i stand til å reagere raskt på organisasjonsendringer, øke engasjementet blant ledere og sette mennesker i sentrum for strategisk planlegging.

 [linkedin.com/company/sympa-hr/](https://www.linkedin.com/company/sympa-hr/)

 [facebook.com/SympaHR/](https://www.facebook.com/SympaHR/)

 [instagram.com/sympahr/](https://www.instagram.com/sympahr/)

