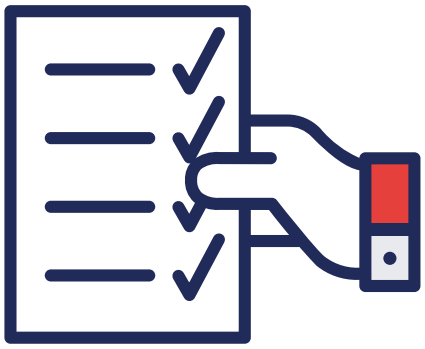

GDPR-tjeklisten til HR

Tjeklisten hjælper dig med at danne dig et overblik over, hvilke systemer I lagrer hvilke data i, og undersøge hvorvidt jeres datalagringspolitik overholder EU-lovgivningen om datasikkerhed.

Dokumentet indeholder også nyttige spørgsmål, som kan hjælpe jer med at finde ud af, om jeres partnere overholder lovgivningen.

Retten til privatliv

Spørgsmål	Hvorfor er det nødvendigt at stille dette spørgsmål?	Ja	Nej	Ved ikke
Er det nemt for jeres **kunder** at anmode om og modtage alle de oplysninger, som I opbevarer om dem?	Personer har ret til at se, hvilke persondata I opbevarer om dem, og hvordan I bruger dem.			
Er det nemt for jeres kunder at få rettet eller opdateret forkerte eller ufuldstændige oplysninger?	Personer har ret til at få foretaget rettelser af forkerte persondata om dem selv.			
Er det nemt for jeres kunder at anmode om at få deres persondata slettet?	Personer har normalt ret til at bede jer om at slette alle de persondata, I opbevarer om dem. I skal kunne opfylde en sådan anmodning inden for omkring en måned.			
Er det nemt for jeres kunder at bede jer om at ophøre med at behandle deres data?	De personer, som I har gemt data om, kan anmode om, at al behandlingen af deres data stoppes eller begrænses midlertidigt, hvis visse betingelser er opfyldt.			
Er det nemt for jeres kunder at modtage en kopi af deres persondata i et format, der nemt kan overføres til en anden virksomhed?	GDPR kræver, at I skal kunne sende personers data i et almindeligt læsbart format enten til dem selv eller til en tredjepart, som de udpeger. Dette repræsenterer grundtanken i GDPR, om at det er personer selv, der ejer deres data, og ikke virksomhederne.			
Er det nemt for jeres kunder at gøre indsigelse mod, at I behandler deres data?	Hvis I behandler deres data med henblik på direkte marketing, skal I straks ophøre med behandlingen af dataene. Hvis dette ikke er tilfældet, kan I muligvis afvise deres indsigelse, hvis I kan påvise legitime grunde til behandlingen.			

Spørgsmål	Hvorfor er det nødvendigt at stille dette spørgsmål?	Ja	Nej	Ved ikke
Hvis I tager beslutninger angående personer på baggrund af automatiserede processer, har I så en procedure til beskyttelse af deres rettigheder?	Hvis I bruger automatiserede processer til at hjælpe med at tage beslutninger, der har en væsentlig betydning for personer, skal I definere en procedure, der sikrer, at I beskytter personers rettigheder. I skal også gøre det nemt for personer at anmode om en personlig vurdering, påvirke beslutninger og udfordre beslutninger, som I allerede har taget.			

Datasikkerhed

Spørgsmål	Hvorfor er det nødvendigt at stille dette spørgsmål?	Ja	Nej	Ved ikke
Er jeres data krypterede, pseudonymiserede eller anonymiserede overalt, hvor dette er muligt?	GDPR kræver, at organisationer bruger kryptering eller pseudonymisering i alle tilfælde, hvor dette er muligt.			
Har I truffet foranstaltninger, der muliggør efterfølgende kontrol og bekræftelse af identiteten på den person, der har registreret, ændret eller overført persondata?	Hvis I oplever et brud på persondatasikkerheden, som er målrettet et informationssystem, er I underlagt et dokumentationskrav, der omfatter at levere informationssystemets logdata fra det tidspunkt, hvor sikkerhedsbruddet skete.			
Har I truffet interne foranstaltninger til at undgå uautoriseret adgang til persondata?	GDPR kræver, at persondata behandles på en måde, der sikrer dataenes fortrolighed i passende grad. Det omfatter at forhindre uautoriseret adgang til eller brug af persondata og det udstyr, der anvendes til behandlingen.			

Spørgsmål	Hvorfor er det nødvendigt at stille dette spørgsmål?	Ja	Nej	Ved ikke
Har I truffet foranstaltninger, der sikrer den løbende fortrolighed, integritet, tilgængelighed og modstandsdygtighed i de behandlingssystemer og tjenester, der er relateret til behandlingen af persondata?	Jeres systemer og software skal være forberedt i tilfælde af databrud. GDPR kræver, at I har mulighed for hurtigt at genoprette tilgængeligheden af og adgangen til persondata i tilfælde af en fysisk eller teknisk hændelse.			
Har I en procedure til regelmæssig test, analyse og evaluering af effektiviteten af jeres tekniske og organisatoriske forholdsregler til sikring af behandlingen?	GDPR kræver, at disse tekniske og organisatoriske forholdsregler skal gennemgås regelmæssigt og opdateres efter behov. Hvis I bruger en Databehandler, skal denne hjælpe jeres organisation med at sikre overholdelse af dette krav.			
Har I fastlagt en proces for, hvordan I giver myndighederne og jeres dataregistrerede besked i tilfælde af et databrud?	Hvis der sker et databrud, og persondata kan være blevet misbrugt, skal I give den tilsynsførende myndighed besked inden for 72 timer. Der er også krav om, at I hurtigt kommunikerer om databrud til jeres dataregistrerede, medmindre det er usandsynligt, at bruddet kan medføre en risiko for dem. Hvis I bruger en Databehandler, skal denne hjælpe jeres organisation med at sikre overholdelse af dette krav.			

Ansvarlighed og forvaltning

Spørgsmål	Hvorfor er det nødvendigt at stille dette spørgsmål?	Ja	Nej	Ved ikke
Har I underskrevet en databeskyttelsesaftale mellem jeres organisation og tredjeparter, der behandler (HR-relaterede) persondata på jeres vegne?	GDPR kræver, at behandling via en databehandler er underlagt en kontrakt. Lovgivningen indeholder en detaljeret liste over ting, som aftalen mellem parterne skal indeholde.			
Hvis jeres organisation ligger uden for EU, har I så udnævnt en repræsentant i et EU-medlemsland?	Hvis I behandler data, der er relateret til personer i en bestemt medlemsstat, skal I muligvis udnævne en repræsentant i det pågældende land, som kan kommunikere på jeres vegne i forhold til databeskyttelsesmyndighederne.			
Har I udnævnt en dataansvarlig?	I tre situationer er der krav om, at organisationer skal have en dataansvarlig, men det er under alle omstændigheder en god ide at have en, selvom denne regel ikke gælder for jer. Den dataansvarlige skal være ekspert i databeskyttelse.			

Lovgrundlag og gennemsigtighed

Spørgsmål	Hvorfor er det nødvendigt at stille dette spørgsmål?	Ja	Nej	Ved ikke
Har I udført en informations audit for at registrere, hvilke informationer I behandler, og hvem der har adgang til dem?	Organisationer, der har mindst 250 medarbejdere eller udfører databehandling med høj risiko, skal vedligeholde en opdateret og **detaljeret liste over deres behandlingsaktiviteter** og være forberedt på at skulle vise denne liste til myndighederne efter anmodning. Organisationer med færre end 250 medarbejdere bør også udarbejde en analyse, da dette vil gøre det nemmere at overholde de øvrige krav i GDPR.			
Har I gennemført en konsekvensanalyse vedrørende databeskyttelse (DPIA)?	GDPR kræver en DPIA, når behandlingsaktiviteten sandsynligvis vil resultere i en høj risiko for virkelige personers rettigheder og frihed. *Hvis I bruger en Databehandler, skal denne hjælpe jeres organisation med at sikre overholdelse af dette krav.*			
Har I angivet tydelige oplysninger om jeres databehandling og de juridiske begrundelser i jeres politik om beskyttelse af personlige oplysninger?	I skal fortælle personer, at I indsamler deres data, og hvorfor I gør det. I skal forklare, hvordan dataene behandles, hvem der har adgang til dem, og hvordan I sikrer dem. Disse oplysninger skal være inkluderet i jeres politik om beskyttelse af personlige oplysninger og leveres til de dataregistrerede på det tidspunkt, hvor I indsamler deres data.			

Sympa's HR-System er udviklet til at overholde GDPR-princippet om "**Databeskyttelse gennem design og som standard**".

sympa.dk