FÖR HR:

# GDPR-checklista

Det här dokumentet hjälper dig att identifiera system där ni lagrar data, samt att ta reda på om er organisations lagringspolicyer ligger i linje med EU:s förordningar gällande dataskydd.

Den här checklistan innehåller även praktiska frågor som hjälper er att avgöra om era samarbetspartner lever upp till kraven i dataskyddsförordningen.

# Sekretessrättigheter

| Fråga | Varför är det viktigt? | Ja | Nej | Vet ej | |
|---|---|---|---|---|---|
| Är det enkelt för era kunder att begära och få tillgång till all information ni lagrar om dem? | Kunder har rätt att se vilka personuppgifter ni lagrar om dem och hur ni använder dem. | | | | |
| Är det enkelt för kunder att rätta eller uppdatera felaktig eller ofullständig information? | Alla kunder har rätt att kunna korrigera felaktiga personuppgifter. | | | | |
| Är det enkelt för era kunder att begära att deras personuppgifter ska raderas? | Alla kunder har i allmänhet rätt att be er radera personuppgifter som ni lagrar om dem. Ni bör kunna uppfylla en sådan begäran inom en månad. | | | | |
| Är det enkelt för kunder att begära att ni slutar bearbeta deras personuppgifter? | Registrerade personer kan begära att ni begränsar eller slutar bearbeta deras information temporärt om vissa skäl föreligger. | | | | |
| Är det enkelt för era kunder att få en kopia på sina personuppgifter i ett format som är lätt att överföra till ett annat företag? | Dataskyddsförordningen (GDPR) kräver att ni ska kunna skicka personuppgifter i ett vanligt läsbart format, antingen direkt till den registrerade personen eller till en tredje part som de utser. Idén i GDPR är att den registrerade personen äger sina personuppgifter, inte företag. | | | | |
| Är det enkelt för kunder att motsätta sig att ni bearbetar deras personuppgifter? | Om ni bearbetar deras personuppgifter i marknadsföringssyfte måste ni omedelbart sluta när kunden motsätter sig. Om ni kan visa att ni har legitima skäl är det möjligt att ni kan bestrida kundens invändning. | | | | |

# Sekretessrättigheter

| Fråga | Varför är det viktigt? | Ja | Nej | Vet ej | |
|---|---|---|---|---|---|
| Om ni fattar beslut om personer baserat på automatiska processer – har ni i så fall en process för att skydda deras rättigheter? | Om ni använder er av automatiska processer för att fatta beslut som kan påverka människor på ett signifikativt sätt måste ni etablera en process för att säkerställa att ni skyddar registrerade personers rättigheter. Ni måste även göra det enkelt för registrerade personer att kunna: begära ett ingripande av en faktisk person, tillhandahålla beslutsunderlag och bestrida beslut som ni redan har fattat. | | | | |

# Datasäkerhet

| Fråga | Varför är det viktigt? | Ja | Nej | Vet ej | |
|---|---|---|---|---|---|
| Är era data krypterade, pseudonymiserade eller anonymiserade när det är möjligt? | GDPR kräver att organisationer använder kryptering eller pseudonymisering när så är möjligt. | | | | |
| Har ni etablerade rutiner som gör det möjligt att kontrollera och verifiera identiteten på den person som har registrerat, ändrat eller överfört personuppgifter? | Om ni drabbas av ett dataintrång i ett informationssystem är ni skyldiga att dokumentera detta med informationssystemets loggdata från tillfället då intrånget inträffade. | | | | |
| Har ni interna rutiner på plats för att förhindra obehörig åtkomst till personuppgifter? | GDPR kräver att personuppgifter behandlas på ett sätt som säkerställer lämplig sekretess, inklusive att förhindra obehörig åtkomst till eller användning av personuppgifter och den utrustning som används för att bearbeta personuppgifter. | | | | |

# Datasäkerhet

| Fråga | Varför är det viktigt? | Ja | Nej | Vet ej | |
|---|---|---|---|---|---|
| Har ni etablerade rutiner för system och tjänster som behandlar personuppgifter för att säkerställa kontinuerlig sekretess, integritet, tillgänglighet och motståndskraft? | Era system och program måste vara förberedda på dataintrång. GDPR kräver att ni har möjlighet att återställa både tillgänglighet och åtkomst till personuppgifter inom en rimlig tidsram vid en fysisk eller teknisk incident. | | | | |
| Har ni etablerade rutiner för att testa, bedöma och utvärdera effektiviteten i tekniska och organisatoriska rutiner för att se till att all bearbetning är säker? | Enligt GDPR ska tekniska och organisatoriska rutiner granskas regelbundet och uppdateras vid behov. *Om ni använder en databehandlare är det upp till dem att se till att det här kravet efterlevs.* | | | | |
| Har ni en etablerad process för att meddela myndigheter och registrerade personer vid ett eventuellt dataintrång? | Om ett dataintrång inträffar och personuppgifter röjs måste ni meddela tillsynsmyndigheten inom 72 timmar. Ni måste även snabbt meddela alla registrerade personer, såvida dataintrånget inte medfört några risker för dem. *Om ni använder en databehandlare är det upp till dem att se till att det här kravet efterlevs.* | | | | |

# Ansvar och styrning

| Fråga | Varför är det viktigt? | Ja | Nej | Vet ej | |
|---|---|---|---|---|---|
| Har ni skriftliga dataskyddsavtal med alla tredje parter som bearbetar (HR-relaterade) personuppgifter å era vägnar? | GDPR kräver att bearbetning av databehandlare styrs av ett avtal. Förordningen innehåller en detaljerad lista med saker som parterna måste vara överens om. | | | | |
| Om organisationen är utanför EU: har ni utsett en representant i ett av EU:s medlemsländer? | Om ni bearbetar personlig information i ett visst medlemsland kan ni behöva utse en representant i det landet som kan kommunicera med dataskyddsmyndigheter å era vägnar. | | | | |
| Har ni utsett ett dataskyddsombud? | I tre olika fall måste organisationer ha ett dataskyddsombud, men det är en bra idé att ha ett dataskyddsombud även om reglerna inte gäller för er organisation. Dataskyddsombudet ska vara expert på dataskydd. | | | | |

# Laglig grund och transparens

| Fråga | Varför är det viktigt? | Ja | Nej | Vet ej | |
|---|---|---|---|---|---|
| Har ni genomfört en informationsgranskning för att avgöra vilken typ av information ni bearbetar och vem som har tillgång till den? | Organisationer som har minst 250 anställda eller som bearbetar data med högre risk måste ha en uppdaterad och detaljerad lista med sina bearbetningsaktiviteter, samt kunna visa denna lista för tillsynsmyndigheter på begäran. Organisationer med färre än 250 anställda bör också genomföra en granskning eftersom det gör det lättare att efterleva andra krav i GDPR. | | | | |
| Har ni genomfört en konsekvensbedömning av dataskydd? | GDPR kräver en konsekvensbedömning när det är sannolikt att bearbetningsaktiviteten medför stora risker för personliga rättigheter och friheter. *Om ni använder en databehandlare är det upp till dem att se till att det här kravet efterlevs.* | | | | |
| Har ni tillhandahållit tydlig information om er databearbetning och juridiska motiveringar i er sekretesspolicy? | Ni måste förklara för kunder och användare att ni samlar in deras information och varför. Ni bör förklara hur data bearbetas, vem som har tillgång till den och hur ni skyddar den. Den här informationen ska vara inkluderad i er sekretesspolicy och ska även tillhandahållas till registrerade personer när ni samlar in deras data. | | | | |

# Om oss

Sympa erbjuder det bästa heltäckande HR-systemet som sömlöst hanterar hela medarbetarresan. Det är globalt, flexibelt och lätt att använda. Sympas omfattande ekosystem gör det även möjligt att integrera alla andra HR-verktyg för en smidig datadelning och överföring av arbetsflöden mellan systemen. Vår plattform är utrustad med unika samarbetsbaserade funktioner som hjälper HR och företagsledarna att snabbt reagera på förändringar i verksamheten, öka chefernas engagemang och sätta medarbetarna i centrum av den strategiska planeringen.

linkedin.com/company/sympa-hr/

facebook.com/SympaHR/

instagram.com/sympahr/

Sympa