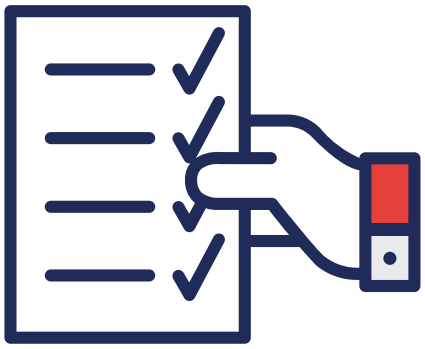
Sympa



HR-tiimin GDPR-muistilista

HR-tiimeille personoitu GDPR-muistilistamme auttaa sinua jäljittämään järjestelmiä, joihin tallennat tietoja ja määrittämään, noudattavatko organisaatiosi tiedonhallinta EU:n säännöksiä tietoturvasta. Olemme lisänneet listaan myös hyödyllisiä kysymyksiä, joiden avulla voit todeta, noudattavatko yhteistyökumppanisi säännöksiä.

Oikeus yksityisyyteen

Kysymys	Miksi tämä on tärkeä kysmys esittää?	Kyllä	Ei	En osaa sanoa
Onko henkilöiden helppoa pyytää ja vastaanottaa kaikkia tietoja, joita sinulla on heistä?	Henkilöillä on oikeus nähdä, mitä henkilötietoja sinulla on heistä ja miten käytät näitä tietoja.			
Onko henkilöiden helppo korjata tai päivittää epätarkkoja tai puutteellisia tietoja?	Henkilöillä on oikeus heitä koskevien virheellisten henkilötietojen oikaisuun.			
Onko henkilöiden helppoa pyytää henkilötietojensa poistamista?	Henkilöillä on oikeus pyytää sinua poistamaan kaikki henkilötiedot, jotka sinulla on heistä. Sinun tulee pystyä noudattamaan tätä pyyntöä suunnilleen kuukauden kuluessa.			
Onko henkilöiden helppoa pyytää sinua lopettamaan tietojensa käsittely?	Rekisteröidyt voivat pyytää rajoittamaan tietojensa käsittelyä tai lopettamaan sen väliaikaisesti tietyillä perusteilla.			
Onko henkilöiden helppoa saada kopio henkilötiedoistaan sellaisessa muodossa, että ne on helppo siirtää toiseen yritykseen?	GDPR vaatii, että henkilötiedot tulee voida lähettää yleisesti luettavassa muodossa joko heille itselleen tai heidän osoittamalleen kolmannelle osapuolelle. Tämä edustaa GDPR:n periaatetta siitä, että henkilöt omistavat omat tietonsa, eivät yritykset.			
Onko henkilöiden helppoa vastustaa tietojensa käsittelyä?	Käsitellessäsi tietoja suoramarkkinointitarkoitukseen, on tietojen käsittely lopetettava heti. Muussa tapauksessa voit ehkä vastustaa heidän vaatimustaan, jos pystyt osoittamaan pakottavat lailliset perusteet tietojen käsittelyyn.			

Kysymys	Miksi tämä on tärkeä kysmys esittää?	Kyllä	Ei	En osaa sanoa
Teetkö henkilöitä koskevia päätöksiä automaattisten prosessien pohjalta? Onko yrityksessä olemassa menettelytapa heidän oikeuksiensa suojaamista varten?	Käyttäessäsi automaattisia prosesseja auttamaan sellaisten päätösten teossa, joilla on merkittäviä vaikutuksia henkilöihin, on laadittava menettelytapa, jolla varmistetaan henkilöiden oikeuksien suojaaminen. Henkilöille on tehtävä helpoksi pyytää ihmisen väliintuloa, arvioida päätöksiä ja valittaa jo tekemistäsi päätöksistä.			

Tietoturva

Kysymys	Miksi kysytään?	Kyllä	Ei	En osaa sanoa
Ovatko keräämäsi tiedot salattuja, pseudonymisoituja tai anonymisoituja aina kun mahdollista?	GDPR vaatii, että organisaatiot käyttävät salausta tai pseudonymisointia aina, kun se on toteutettavissa.			
Onko yrityksessä käytössä menetelmiä, joilla henkilö, joka on tallentanut, muuttanut tai siirtänyt henkilötietoja, voidaan tarkistaa ja todentaa myöhemmin?	Kohdatessasi henkilötietojen tietosuojaloukkauksen, joka on kohdistettu tietojärjestelmään, sinulla on dokumentointivelvollisuus, joka sisältää tietojärjestelmän lokitietojen toimittamisen loukkauksen ajankohdasta.			
Onko yrityksessä käytössä sisäisiä menetelmiä, joilla estetään henkilötietojen luvaton käyttö?	GDPR edellyttää, että henkilötietoja käsitellään tavalla, joka varmistaa tietojen asianmukaisen luottamuksellisuuden. Tähän kuuluu, että estetään luvaton pääsy henkilötietoihin ja niiden käsittelyyn käytettäviin laitteisiin.			

Kysymys	Miksi kysytään?	Kyllä	Ei	En osaa sanoa
Onko yrityksessä käytössä toimenpiteitä, jotka varmistavat käsittelyjärjestelmien ja henkilötietojen käsittelyyn liittyvien palvelujen jatkuvan luottamuksellisuuden, eheyden, saatavuuden ja häiriönsietokyvyn?	Järjestelmien ja ohjelmistojen täytyy olla suojattuja tietomurtoja vastaan. GDPR vaatii, että henkilötietojen saatavuus ja niiden käyttö voidaan palauttaa viipymättä, mikäli on tapahtunut fyysinen tai tekninen häiriötilanne.			
Onko yrityksessä olemassa prosessi, jolla testataan ja arvioidaan säännöllisesti teknisten ja hallinnollisten toimenpiteiden tehokkuutta henkilötietojen käsittelyn turvallisuuden varmistamiseksi?	GDPR määrää, että tekniset ja hallinnolliset toimenpiteet tulee tarkastaa säännöllisesti ja päivittää tarvittaessa. *Jos yrityksessä on käytössä henkilötietojen käsittelijä, tämän tulee auttaa organisaatiota varmistamaan, että velvoitetta noudatetaan.*			
Onko yrityksessä käytössä prosessi, jolla ilmoitetaan viranomaisille ja rekisteröidyille tietosuojaloukkauksesta?	Tietomurron tai tietosuojaloukkaus tapauksissa jossa henkilötietoja on paljastunut, onilmoitettava valvontaviranomaiselle 72 tunnin sisällä. Tietosuojaloukkauksista on myös ilmoitettava nopeasti rekisterissä olleille henkilöille, paitsi jos on epätodennäköistä, että loukkaus asettaa heidät vaaraan. *Jos yrityksessä on käytössä henkilötietojen käsittelijä, tämän tulee auttaa organisaatiota varmistamaan, että velvoitetta noudatetaan.*			

Osoitusvelvollisuus ja hallinta

Kysymys	Miksi kysytään?	Kyllä	Ei	En osaa sanoa
Oletko allekirjoittanut tietosuojasopimuksen organisaatiosi ja kolmansien osapuolten välillä jotka käsittelevät (HR:ään liittyviä) henkilötietoja puolestasi?	GDPR vaatii, että henkilötietojen käsittelijän suorittamaa käsittelyä hallitaan sopimuksella. Asetus sisältää yksityiskohtaisen luettelon seikoista, joista osapuolten on sovittava.			
Sijaitseeko organisaatiosi EU:n ulkopuolella? Oletko nimittänyt edustajan henkilötietojen käsittelylle jostain EU:n jäsenvaltiosta?	Käsitellessäsi tietoa, jotka koskevat henkilöitä jossain tietyssä jäsenvaltiossa, voi olla tarpeen nimetä kyseisestä maasta edustaja, joka voi keskustella puolestasi tietosuojaviranomaisten kanssa.			
Oletko nimennyt tietosuojavastaavan?	Organisaatiolta vaaditaan tietosuojavastaavan nimeämistä (Data Protection Officer, DPO) kolmessa tilanteessa, mutta on kuitenkin hyödyllistä nimittää sellainen, vaikka määräys ei koskisikaan sinua. Tietosuojavastaavan tulee olla tietosuojan asiantuntija.			

Lakiperusteet ja läpinäkyvyys

Kysymys	Miksi kysytään?	Kyllä	Ei	En osaa sanoa
Oletko tarkistanutmitä tietoja käsittelette ja kenellä on pääsy niihin?	Organisaatioilta, joissa on vähintään 250 työntekijää tai joissa suoritetaan suuren riskin henkilötietojen käsittelyä, edellytetään ajantasaisen ja **yksityiskohtaisen luettelon pitämistä henkilötietojen käsittelytoimenpiteistä** ja valmiutta esittää tämä luettelo valvojille pyynnöstä. On suositeltavaa että organisaatioiden, joissa on alle 250 työntekijää, suorittaisivat myös arvioinnin, koska se helpottaa GDPR:n muiden vaatimusten täyttämistä.			
Oletko suorittanut tietosuojaa koskevan vaikutustenarvioinnin (DPIA)?	Yleinen tietosuoja-asetus edellyttää vaikutustenarvioinnin (DPIA:n) tekemistä, kun käsittelyn aikana on vaarana, että se voi aiheuttaa suuren riskin luonnollisten henkilöiden oikeuksille ja vapauksille.. *Jos käytössä on henkilötietojen käsittelijä, tämän tulee auttaa organisaatiota varmistamaan, että velvoitetta noudatetaan.*			
Oletko antanut tietosuojaselosteessa selkeää tietoa kuinka henkilötietoja kätiellään ja sen laillisista perusteista?	Sinun on kerrottava henkilöille, että keräät heidän tietojaan ja miksi tietoa kerätään. Sinun on avattava, miten tietoja käsitellään, kenellä on pääsy niihin ja millä tavoin pidät ne suojattuina. Edellämainitut tiedot tulee sisällyttää yrityksen tietosuojaselosteeseen ja toimittaa henkilöille sillä hetkellä, kun heidän henkilötietojaan kerätään.			

Sympan HR-ohjelmisto on luotu
täyttämään GDPR:n vaatimukset
**“Lähtökohtaisesti suunniteltu jo
tietosuoja -periaatteen mukaisesti”.**

sympa.com