phorest

Opas kampaamoille ja kauneushoitoloille:

Valmistaudu EU:n uuteen tietosuoja-asetukseen

GDPR

www.salonGDPR.fi

Sisällys

LUKU 1: Opi GDPR:stä

1 Johdatus GDPR:ään
2 Mihin tietoihin GDPR vaikuttaa kampaamossa tai hoitolassa?
3 Kuka on vastuussa mistäkin?

LUKU 2: GDPR:n vaatimuksiin vastaaminen

4 Kuinka vastata GDPR:n vaatimuksiin
5 Tilivelvollisuus
6 Suostumus
7 Yksilön oikeudet
8 GDPR-koulutus
9 Lapset kampaamossasi tai hoitolassasi
10 Asiakkaiden pääsy omiin henkilötietoihinsa

Takakansi: Kuinka Phorest voi auttaa

11 Kuinka Phorest voi auttaa sinua vastaamaan GDPR:n vaatimuksiin paremmin

Tärkeää. Tämä kirja on tarkoitettu ainoastaan ohjeistukseksi, eikä sisällä oikeudellista neuvontaa tai analyysiä. Kaikkien tietoja käsittelevien ja hallitsevien organisaatioiden tulee tietää tietosuoja-asetuksen (GDPR) koskevan heitä. Vastuu asetukseen tutustumisesta on kampaamolla tai hoitolalla itsellään. Tämä opas on tarkoitettu ainoastaan alkuun pääsemiseksi. Yritykset voivat joutua hakemaan oikeudellista neuvontaa itsenäisesti arvioidessaan tai kehittäessään omaa prosessiaan ja toimintatapojaan tai käsitellessään oikeudellisia kysymyksiä.

Luku 1 - OPI GDPR:stä

1 Johdatus GDPR:ään

Luultavasti olet jo kuullut kirjaimet GDPR esimerkiksi tapahtumissa, netissä ja eri medioissa. GDPR on lyhenne sanoista General Data Protection Regulation ja tarkoittaa suomeksi uutta EU:n yleistä tietosuoja-asetusta. GDPR astuu voimaan toukokuussa 2018. Tämä opas sisältää tietoa, jonka tarkoituksena on auttaa sinua valmistautumaan GDPR:ään ja hallitsemaan muutosta sinun asiakkaidesi, tiimisi ja yrityksesi menestyksen parhaaksi. Toivomme, että voimme auttaa sinua tässä.

Mikä on GDPR ja miksi se vaikuttaa minun liiketoimintaani?

GDPR on uusi tietolainsäädäntö joka astuu voimaan toukokuussa 2018 ympäri Eurooppaa. Sen tarkoitus on luoda kuluttajien henkilötietojen suojaukseen yhtenäinen toimintamalli EU:n jäsenmaihin. Sen on tarkoitus myös tuoda läpinäkyvyyttä siihen, kuinka yritykset säilyttävät ja käyttävät yksilöiden henkilötietoja.

Tämä on erityisen mielenkiintoista hius- ja kauneudenhoitoalalla, sillä liikkeissä kerätään niin paljon henkilökohtaisia tietoja yhteystiedoista allergioihin ja lääkitykseen.

Tämän takia meidän täytyy yhdessä valmistautua ja saada kaikki kuntoon alusta alkaen. Älä huoli, me opastamme sinua!

On olemassa jo paljon tietosuojalakeja, miksi huolia tästä?

GDPR on laajempi kuin yksikään muu tietosuojalaki. On muutama syy, joiden takia sinun tulisi kiinnittää erityisesti huomiota siihen:

> Sinua voidaan sakottaa jopa 4% liikevaihdostasi 20 miljoonaan saakka, eli jos liikevaihtosi on 385 000 euroa, voit joutua maksamaan yli 15 000 euron sakon.

> Lähempänä tietosuoja-asetuksen voimaan astumista EU rohkaisee jokaista jäsenmaata tiedottamaan siitä yleisissä tiedotusvälineissä. Tällä EU haluaa saada kansalaiset tietoisiksi oikeuksistaan tilanteissa, joissa yritykset (kuten liikkeesi) käyttää heidän henkilötietojaan. Tämä tulee lisäämään kuluttajien tietoisuutta ja sinun täytyy suojata liiketoimintaasi olemalla valmiina vastaamaan asiakkaidesi kysymyksiin ja todistamaan, että käsittelet heidän tietojaan turvallisesti ja GDPR:n mukaisesti.

Kuulostaa paljolta työltä, ja hieman pelottavalta…

GDPR on monimutkainen säädös, mutta meillä on myös hyviä uutisia. Ensinnäkin, me olemme täällä auttamassa sinua saavuttamaan GDPR-valmiuden (katso takakansi)!

Lisäksi, liikkeet, jotka noudattavat asetusta toukokuuhun mennessä ovat etulyöntiasemassa. Heidän asiakkaansa nimittäin tietävät henkilötietojensa olevan turvassa, eikä käytössä jatkuvaa markkinointia varten tai minkään kolmannen osapuolen toimesta.

Ne liikkeet, jotka ovat hyvin valmistautuneita, voivat hyödyntää valmiuttaan myös lisäämällä luottamusta ja uskoa siihen, kuinka paljon he välittävät asiakkaistaan ja näiden henkilötiedoista.

2 Mihin tietoihin GDPR vaikuttaa kampaamossa tai hoitolassa?

GDPR vaikuttaa lähinnä henkilötietoihin. Mutta mitä henkilötiedot tarkalleen on kampaamoissa ja kauneushoitoloissa?

> Kaikki tiedot jotka liittyvät tiettyyn henkilöön, esimerkiksi nimi, syntymäpäivä, henkilötunnus, osoite ja terveyteen liittyvät tiedot

> Puhelinnumerot ja kuvat, joista henkilön voi tunnistaa, lasketaan myös henkilötiedoiksi

> Terveyteen liittyvät tiedot, kuten ihosairaudet tai lääkitys, ovat arkaluontoisia tietoja ja niitä täytyy käsitellä erityisen huolellisesti. On elintärkeää, että koko liikkeesi henkilöstö ymmärtää taloudelliset ja maineeseen liittyvät seuraukset, joihin tietojen väärä käsittely voi johtaa.

Eli kuten näet, keräät jo nyt paljon tietoja, joihin GDPR vaikuttaa!

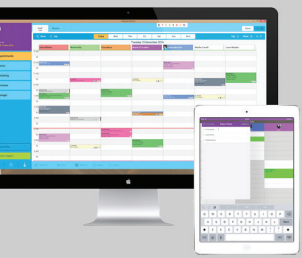
3 Kuka on vastuussa mistäkin?

GDPR:n mukaan tietojen suojauksesta on vastuussa kaksi pääasiallista osapuolta - rekisterinpitäjä ja tietojen käsittelijä.

Kampaamona tai kauneushoitolana sinä olet rekisterinpitäjä. Sinä keräät tietoja ja päätät, kuinka niitä kerätään ja kuinka kerättyjä tietoja käytetään hoidoissa, värjäystöissä, markkinoinnissa, tuotemyynnissä jne. Toisin sanoen sinä teet päätökset siitä, kuinka asiakkaidesi henkilötietoja tulisi kerätä ja käyttää.

Phorest on tietojen käsittelijä, sillä se on työkalu, joka auttaa sinua pitämään rekisteriä. Liikkeet, jotka käyttävät järjestelmäämme, käyttävät sitä kerätäkseen ja käsitelläkseen henkilötietoja.

TÄMÄN TAKIA ON **ERITTÄIN TÄRKEÄÄ** KÄYTTÄÄ GDPR:ÄÄ NOUDATTAVAA JÄRJESTELMÄÄ.



4 Kuinka vastata GDPR:n vaatimuksiin?

Jotta voisit toimia GDRP:n mukaisesti, yrityksesi täytyy todentaa asiakkaiden henkilötietojen keräämiselle olevan laillisia perusteita. Tämä tarkoittaa, että et voi kerätä henkilötietoja ilman syytä, tai sanoa ympäripyöreästi tietojen olevan esimerkiksi markkinointia varten (lisää tästä myöhemmin kohdassa 'Suostumus').

Sinun täytyy pystyä:

> Todentamaan tarkalleen, mitä henkilötietoja keräät

> Antamaan laillinen peruste tiedon keräämiselle. Esimerkiksi syy allergioiden kysymiseen voi olla lapputestien tekeminen

> Näyttämään, että kaikki datankeräysprosessisi ovat tietosuoja-asetuksen mukaisia. Esimerkiksi asiakkaasi tehdessä valituksen viranomaisille, sinun täytyy pystyä todistamaan yksityskohtaisesti, kuinka olet kerännyt, säilyttänyt ja käyttänyt heidän tietojaan.

5 Tilivelvollisuus

Aiempien vaatimusten lisäksi tarvitset ennakoivan lähestymistavan näyttää noudattavasi tietosuojaa, etkä vain kykyä peittää jälkiäsi esimerkiksi tarkastuksen tai asiakkaan valituksen yhteydessä.

Jotta voisit osoittaa toimivasi säädösten mukaan, tarvitset dokumentteja, kuten esimerkiksi tietosuojaa ja tietojen käsittelyä koskevia menettelykäsikirjoja. Näitä vaaditaan tarkastusten yhteydessä.

Kaikista tärkeintä on, että **sinulla täytyy olla asiakkaan suostumuksesta dokumentti, joka todistaa että asiakas on valinnut luovuttavansa sinulle tietojansa.** Lisäksi seuraavien yksityiskohtien tulee olla saatavilla koskien tarkasteltavia tietoja:

- Miksi sinulla on tiedot?
- Kuinka hankit ne?
- Minkä takia hankit ne?
- Onko tiedot turvassa? Kenellä on pääsy niihin?
- Missä säilytät tietoja?
- Tarvitsetko tietoja vielä? Kuinka pitkään aiot säilyttää niitä?
- Onko kolmansilla osapuolilla pääsyä tietoihin?

6 Suostumus

Olet luultavasti syöttänyt tietosi nettilomakkeelle saadaksesi uutiskirjeen tai tuote-esittelyn… ehkä jopa Phorestin esittelyn!

Aiemmin yritysten kerätessä tietoja oli hyväksyttävää, että lomakkeen tai nettisivun alareunassa oli rastitettava ruutu ja teksti 'haluan vastaanottaa markkinointia, tarjouksia ja uutisia kampaamostasi'. Voi olla, että olet myös nähnyt esimerkkejä valmiiksi rastitetuista ruuduista, joita täytyi klikata jotta ei vastaanottaisi markkinointia. GDPR:n astuessa voimaan tämän täytyy muuttua.

> Olet velvoitettu kertomaan selkeästi keräämiesi tietojen käsittelyprosessin, eli mihin tietoja tarkalleen tullaan käyttämään. Yksi ympäripyöreä toteamus käyttötarkoituksesta ei ole hyväksyttävä.

> Et voi pyytää asiakkailtasi suostumusta rastittamalla valintaruutuja valmiiksi. Heidän täytyy antaa suostumuksensa rastittamalla ruutu itse. Sinulla täytyy olla tositteita siitä, kuinka tiedot on kerätty ja että asiakas on nimenomaan valinnut luovuttaa tietonsa

> Asiakkailla tulee olla mahdollisuus pyytää, että KAIKKI heidän tietonsa poistetaan.

> Sinulla täytyy olla jälkitallennus siitä, miten tiedot oli kerätty ja asiakkaiden suostumukset saatu.

7 Yksilön oikeudet

Tietosuojan periaate on se, että henkilötiedot kuuluvat aina tietojen kohteelle, riippumatta siitä kenen kanssa ne jaetaan.

Asiakkaillasi tulee olemaan KAIKKI alla luetellut oikeudet GDPR:n astuessa voimaan ja sinun täytyy ylläpitää niitä toimiaksesi asetuksen mukaisesti:

A. Oikeus tulla informoiduksi. Asiakkaille täytyy tiedottaa ennen kun henkilötietoja kerätään. Asiakkaan täytyy valita luovuttavansa tietoja ja sinun täytyy tarjota syyt henkilötietojen keräämiselle.

B. Oikeus päästä tietoihin käsiksi. Asiakkailla on oikeus pyytää pääsyä omiin henkilökohtaisiin tietoihinsa ja tietoon siitä, kuinka heidän henkilötietojaan käytetään keräämisen jälkeen.

C. Oikeus tietojen korjaukseen. Asiakkailla on oikeus saada tietonsa korjatuksi mikäli ne ovat vanhentuneita, epätosia tai puuttellisia.

D. Oikeus tulla unohdetuksi. Jos henkilö ei ole enää asiakas tai peruu suostumuksensa henkilötietojensa käyttöön, hänellä on oikeus saada kaikki henkilötietonsa poistetuksi rekisteristä.

E. Oikeus tietojen siirtoon. Asiakkailla on oikeus pyytää, että siirrät heidän henkilötietonsa toiselle yritykselle yleisesti käytetyssä, lukukelpoisessa muodossa.

F. Oikeus vastustaa tietojen käyttöä ja suoramarkkinointia. Asiakkaat voivat vaatia, että heidän henkilötietojaan ei saa käyttää. Heidän tietojaan saa siis säilyttää, mutta ei käyttää.

G. Oikeus vastaanottaa ilmoituksia. Asiakkailla on oikeus saada ilmoitus, mikäli heidän tietojensa tietosuojaa rikotaan. Heidän tulee saada ilmoitus 72 tunnin sisällä siitä, kun tietosuojarikkomus huomataan.

8 GDPR-koulutus

Tämä opas antaa sinulle yleiskatsauksen GDPR:stä, mutta sinun täytyy ymmärtää tätä lainsäädäntöä kokonaisvaltaisesti ja suosittelemmekin, että etsit sinulle ja tiimillesi koulutusta aiheesta GDPR-asiantuntijan taholta. Tietämättömyys ei kelpaa puolustukseksi GDPR:ää rikottaessa.

Tämä lainsäädäntö täytyy ottaa huomioon jatkossa, kun teet päätöksiä liiketoiminnastasi. GDPR:n noudattaminen ei ole kertamuutos, vaan jatkuva prosessi.

Kun hankit tiimillesi koulutusta, sinun kannattaa nimetä joku tiimistäsi liikkeen GDPR-vastaavaksi, joka sisäistää asetuksen täysin ja osaa ohjeistaa ja auttaa muita tiimin jäseniä pääsemään samaan. Tämän henkilön tehtävä olisi siis huolehtia, että kaikki tiimisi jäsenet ymmärtäisivät ja osaisivat toimia säännösten mukaisesti. Tässä on myös loistava tilaisuus ylennykselle, mikäli sinulla on todella omistautunut työntekijä vastaanottotiskilläsi!

Inhimilliset erehdykset aiheuttavat suurimman osan tietoturvarikkomuksista. Esimerkkejä tästä on asiakkaiden tietoja koskevien papereiden käsittelyvirheet, salaamattomia henkilötietoja sisältävien kannettavien tietokoneiden kadottaminen ja sähköpostien lähettäminen väärälle henkilölle.

9 Lapset kampaamossasi tai hoitolassasi

Lapsia pidetään erityisasemassa ja GDPR tarjoaa heille lisäsuojaa. Asetuksen mukaan lapsiksi lasketaan kaikki alle 16-vuotiaat, mutta maat saavat itse säätää tätä ikärajaa 13 ja 16 ikävuoden välillä.

Lapsen ja vanhemman tai huoltajan suostumus täytyy saada, ennen kuin kerätään mitään lapsen henkilötietoja. Koska terveyttä koskevat tiedot ovat arkaluontoisia henkilötietoja ja niihin pätee ylimääräiset rajoitukset, kampaamoiden ja kauneushoitoloiden suositellaan välttämään sellaisten palveluiden tarjoamista alaikäisille, jotka vaatisivat terveystietojen keräämistä.

Tällaisia palveluita alaikäisille tarjoavien kampaamoiden ja hoitoloiden tulisi hakea ammattilaiselta lisäohjeistusta asian suhteen. On hyvä käytäntö suunnitella lomakkeita erityisesti alaikäisten ajanvarauksia varten varmistaaksesi, että toteutat lisäkäytäntöjen noudattamisen.

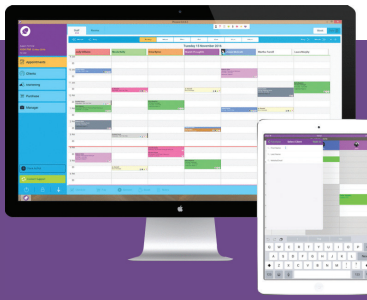
Phorest-järjestelmään on sisällytetty muiden lomakkeiden lisäksi GDPR:ää mukailevia lapsille kohdennettuja lomakkeita!

10 Asiakkaiden pääsy omiin henkilötietoihinsa

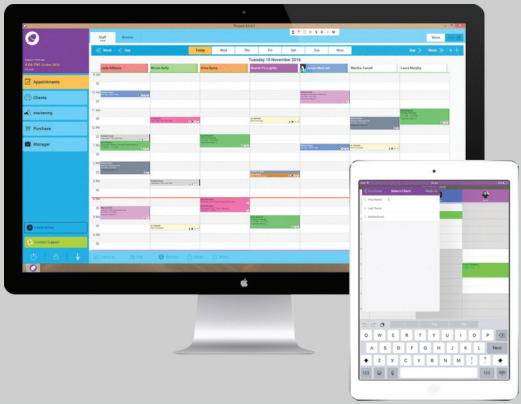
GDPR:n nojalla asiakkaasi voivat pyytää pääsyä omiin tietoihinsa (englanniksi Subject Access Request eli SAR) ja se tarkoittaa, että sinun täytyy tarjota asiakkaallesi ilmaiseksi KAIKKI häntä koskevat tiedot joita säilytät 30 päivän kuluessa.

Toimittaessasi asiakkaasi tietoja sinun täytyy sisällyttää ainakin seuraavat tiedot (muiden tietojen lisäksi):

- Kaikki terveyttä koskevat tiedot, yhteystiedot yms. henkilötiedot
- Miksi säilytät tietoja
- Kaikki siitä, mihin tietoja on käytetty ja tullaan käyttämään
- Henkilöt, joille olet lähettänyt tai joiden kanssa olet jakanut tiedot (asiakkaan suostumuksella)
- Miten tiedot on kerätty
- Kopio asiakkaan antamasta suostumuksesta
- Kuinka pitkään olet säilyttänyt tietoja ja kuinka pitkään aiot säilyttää tietoja, mikäli asiakas on pyytänyt oikeutta tulla unohdetuksi.



Tämä on täydellinen esimerkki siitä, miksi tarvitset GDPR:ää noudattavan järjestelmän.



Phorest voi auttaa sinua saavuttamaan GDPR-valmiuden!

Phorest voi auttaa sinua:

> **SUOSTUMUKSEN KANSSA:** Tarjoamalla ensimmäisenä toimialallaan GDPR:ää noudattavia digitaalisia konsultaatiolomakkeita, joiden avulla asiakkaasi valitsee tietojensa luovuttamisesta GDPR:n mukaisesti.

> **MARKKINOINNISSA:** Tarjoamalla sinulle suodattimia ja työkaluja luoda markkinointikampanjoita sähköpostiin, sosiaaliseen mediaan ja tekstiviesteillä, asiakkaidesi suostumuksella niin, että et joudu hankaluuksiin asiakkaidesi pyytäessä kopiota suostumuksestaan!

> Kaikki tiedot, joita säilytetään Phorest-järjestelmässä on täysin salattuja. Se tarkoittaa, että sinä ja tiimisi suojaatte asiakkaidesi tietoja vuodoilta!

Ota yhteyttä Phorest-tiimiimme jo tänään niin kerromme, kuinka voimme auttaa sinua vastaamaan tietosuoja-asetuksen vaatimuksiin!

Let's Grow!

PUH. 045 189 4881

www.phorest.fi