Datum: 13/02/19

AKKOORDVERKLARING VOOR HET BEWAREN EN GEBRUIKEN VAN PERSOONLIJKE GEGEVENS

Vanaf 1 mei 2018 gaat er een nieuwe wetgeving ter bescherming van uw gegevens van kracht. Deze nieuwe Europese privacy wetgeving genaamd de General Data Protection Regulation (GDPR) zorgt ervoor dat uw gegevens veilig bewaard worden, u zelf de mogelijkheid heeft om uw persoonlijke gegevens te beheren en zelf te bepalen voor welke doeleinden deze gebruikt worden.

Schoonheidssalon La Perla beschikt over o.a. uw e-mailadres, persoonlijk adres en telefoongegevens die bewaard worden in ons klantensysteem. Deze verzamelde gegevens worden enkel gebruikt voor onze commerciële doeleinden en worden niet openbaar gemaakt naar externe bedrijven toe. Om verder met u te kunnen blijven communiceren zoals we tot nu toe gedaan hebben (email, promoties, nieuwsbrieven,…) moet u ons hier echter expliciet toestemming voor geven. Om dit zo eenvoudig mogelijk te maken, hebben we hieronder een elektronisch invulformulier voorzien, waar u kan aanvinken welke informatie u van ons wenst te ontvangen en u daarna uw handtekening kan toevoegen.

Van de Veire Evi respecteert deze wetgeving en heeft tijd tot 30 april 2018 om dit in orde te brengen. Wij vragen u daarom om dit formulier ASAP elektronisch en ingevuld terug te zenden naar info@schoonheidssalon-laperla.be of schriftelijk naar Schoonheidssalon la Perla, Natiënlaan 176, 8300 Knokke. Vanaf 1 mei zal u van ons geen informatie meer ontvangen zonder dit vervolledigd document.

Bedankt voor uw begrip en uw snelle reactie !

BIJLAGE : Informatie omtrent de General Data Protection Regulation (GDPR-wetgeving)

Gelieve onderstaande gegevens te controleren en/of aan te passen:

VOORNAAM ACHTERNAAM _____

ADRES _____

POSTCODE + REGIO _____

LAND _____

TELEFOONNUMMER _____

E-MAILADRES _____

Ik wens volgende e-mails te ontvangen van _____ (vink aan):

☐ Nieuwsbrief
☐ Promoties
☐ Algemene informatie

Ik verklaar hierbij dat ik de privacy wetgeving en de GDPR-wetgeving aandachtig gelezen heb en vervolgens op de hoogte ben van mijn rechten en de mogelijke risico's. Ik geef hierbij mijn toestemming dat _____ mijn persoonlijke gegevens mag bewaren en hiermee gebruik mag maken voor commerciële doeleinden.

Gelezen en goedgekeurd
Naam, voornaam, handtekening

BIJLAGE: INFORMATIE OMTRENT DE GENERAL DATA PROTECTION REGULATION (GDPR-WETGEVING)

General Data Protection Regulation

GDPR (of ook Algemene Verordening Gegevensbescherming – AVG genoemd) gaat over het beheer en de beveiliging van persoonlijke gegevens van Europese burgers. Als organisatie moet u vanaf mei 2018 kunnen aantonen welke persoonsgegevens u verzamelt, hoe u deze data gebruikt en hoe u ze beveiligt (of u dit nu in uw datacenter of in de cloud buiten de EU beheert).

GDPR in het kort:

- Bescherming van persoonlijke data van de Europese burger
- Maatregelen tegen hackers en datalekken
- In voege op 25 mei 2018
- Procedure voor dataverzameling en -opslag van persoonlijke gegevens
- Toestemming vragen om gegevens te verzamelen en gebruiken
- Individu heeft het recht om 'vergeten te worden'
- Verhoogde security maatregelingen zijn nodig
- Datalek moet u kunnen melden binnen 72 uur
- De Nationale Autoriteiten kunnen boetes toepassen
- In grote organisaties moet een DPO (Data Protection Officer) aangesteld worden

Basisbeginselen van de gegevensbescherming

De basisbeginselen zijn de kern van de gegevensbescherming. Ze bestaan al in het huidig recht maar worden in de AVG aanzienlijk versterkt. Iedere verwerkingsverantwoordelijke moet deze beginselen eerbiedigen.

Rechtmatige, behoorlijke en transparante verwerking

Dit beginsel leert ons dat de gegevens rechtmatig, behoorlijk en transparant moeten worden verwerkt ten aanzien van de betrokkene.

Overweging 30 verduidelijkt het begrip transparantie: het moet voor de individuen perfect duidelijk zijn dat hun gegevens zijn ingezameld, gebruikt, geraadpleegd of anders verwerkt. Het transparantiebeginsel vereist dat alle informatie of communicatie met betrekking tot een gegevensverwerking gemakkelijk toegankelijk is en gemakkelijk te begrijpen is.

Er moet dus gebruik gemaakt worden van een duidelijke en eenvoudige taal. Dit gaat vooral over de informatie over de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking. Dit gaat eveneens over de bijkomende informatie die kan verstrekt worden zodat een gerechtvaardigde en transparante verwerking verzekerd is. De individuen moeten verwittigd worden van de risico's, de regels, garanties en rechten die verband houden met de verwerking alsook de manier om hun rechten uit te oefenen.

Dit beginsel is verbonden met artikel 6 van de verordening dat de redenen opsomt waarop een verwerking kan berusten. Dit artikel bepaalt de grondslagen waarop kan worden beoordeeld of een verwerking al dan niet rechtmatig is. U vindt meer informatie over dit artikel 6 onder het punt over de rechtmatigheid van de verwerking.

Juistheid

De gegevens moeten juist zijn en zo nodig worden bijgewerkt. Alle redelijke maatregelen moeten worden genomen om onnauwkeurige of onvolledige gegevens die – uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt – uit te wissen of te verbeteren.

Integriteit en vertrouwelijkheid

De gegevens moeten volgens een afdoend veiligheidsniveau worden verwerkt door gebruik te maken van passende, technische en organisatorische maatregelen.

Dit houdt een bescherming in tegen iedere niet toegelaten of onwettige verwerking, tegen verlies, vernietiging of kwaliteitsverlies van de gegevens.

Overweging 39 verduidelijkt dat de gegevens moeten worden verwerkt op een wijze die instaat voor afdoende veiligheid en vertrouwelijkheid van de gegevens. Dit betekent dat iedere niet toegelaten toegang of gebruik van de gegevens of uitrusting die voor de verwerking wordt aangewend, moet worden voorkomen.

Wat verandert er?

Het feit dat dat moet worden ingestaan voor de veiligheid van de verwerkingen, bestond reeds in de Richtlijn 95/46 maar werd niet vernoemd als basisbeginsel van de gegevensbescherming. We zien een wijziging in het concept gegevensbescherming, dat technischer is geworden.

Welbepaald doeleinde

Dit basisbeginsel bepaalt dat de persoonsgegevens moeten worden verkregen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en niet verder mogen worden verwerkt op een manier die onverenigbaar is met die doeleinden.

De verdere verwerking van persoonsgegevens voor archiveringsdoeleinden voor openbaar belang, voor historisch of wetenschappelijk onderzoek of voor statistische doeleinden, wordt overeenkomstig artikel 89.1 van de AVG, niet beschouwd als onverenigbaar met de oorspronkelijke doeleinden.

Het doelbindingsprincipe bestaat reeds in het huidige recht.

Wat verandert er?

De AVG machtigt in artikel 6.4 de verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, maar enkel als die verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld. In dat geval is er geen andere afzonderlijke rechtsgrond vereist dan die op grond waarvan de verzameling van persoonsgegevens werd toegestaan.

Om na te gaan of een doel van verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld, moet de verwerkingsverantwoordelijke, nadat hij aan alle voorschriften inzake rechtmatigheid van de oorspronkelijke verwerking heeft voldaan, een verenigbaarheidsoefening uitvoeren.

Het is de bedoeling om de verwerkingsverantwoordelijke in staat te stellen om zelf te beoordelen of het hergebruik van persoonsgegevens voor andere doeleinden, al dan niet verenigbaar is.

Daartoe zal rekening moeten worden gehouden met:

- het eventueel bestaan van een verband tussen de doeleinden waarvoor de gegevens werden verkregen en de doeleinden van de voorgenomen verdere verwerking;
- de context waarin de persoonsgegevens werden verkregen, in het bijzonder gelet op de relatie tussen de betrokkenen en de verantwoordelijke voor de verwerking;
- de aard van de persoonsgegevens, vooral als de verwerking slaat op bijzondere categorieën persoonsgegevens, overeenkomstig artikel 9, of als de gegevens betreffende veroordelingen en strafrechtelijke inbreuken worden verwerkt overeenkomstig artikel 10;
- de mogelijke gevolgen van de voorgenomen, verdere verwerking voor de betrokkenen;
- het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

Wanneer echter de betrokkene zijn toestemming heeft gegeven of wanneer de verwerking gebaseerd is op Unierecht of lidstatelijk recht, mag de verwerkingsverantwoordelijke de persoonsgegevens verder verwerken, ongeacht of dat verenigbaar is met de doeleinden.

Minimale gegevensverwerking

Volgens het beginsel van de minimale gegevensverwerking moeten persoonsgegevens toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor het doeleinde waarvoor de gegevens worden verwerkt.

Het is hier de bedoeling dat de verwerkingsverantwoordelijke uitsluitend die gegevens verwerkt die noodzakelijk zijn voor de vastgestelde doeleinden. Verwerk dus enkel het strikte minimum.

Overweging 39 brengt meer duidelijkheid: dit beginsel vereist met name dat de verwerkingsverantwoordelijke er voor instaat dat de bewaartermijn van de gegevens tot een strikt minimum beperkt wordt. De persoonsgegevens mogen maar worden verwerkt als het doeleinde van de verwerking niet op een andere manier kan worden gerealiseerd.

Dit beginsel had in de Richtlijn 95/46 niet deze naam maar het bestond wel al.

Beperkte bewaartermijn

De gegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren en niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt.

De gegevens kunnen voor een langere periode worden bewaard indien ze uitsluitend worden verwerkt voor archiveringsdoeleinden voor openbaar belang, voor historisch of wetenschappelijk onderzoek of voor statistische doeleinden. Deze verwerking moet in overeenstemming zijn met artikel 89 van de AVG.

U moet dus de bewaartermijn van de gegevens die u verwerkt duidelijk vaststellen en mechanismen invoeren waarmee u kunt verifiëren of de persoonsgegevens wel degelijk ontoegankelijk geworden zijn nadat de vastgestelde bewaartermijn is afgelopen.