SIEMBURG
Stichting Dorpshuis Kruisland

Algemene Verordening Gegevensbescherming (AVG)

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.
De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR).

Opgemaakt: 23-05-2018
Evaluatie: 23-05-2021

SIEMBURG
Stichting Dorpshuis Kruisland

Inleiding

Op 25 mei 2018 zal een nieuwe wet rondom privacy en beveiliging van gegevens gaan gelden, de Algemene Verordening Gegevensbescherming (AVG). De wet wordt van kracht zodat in heel Europa dezelfde bepalingen gelden als het gaat om privacy en beveiliging van gegevens.

Deze wet heeft ook gevolgen voor Siemburg omdat de privacyrechten worden uitgebreid. Ook bij Siemburg werken we met persoonlijke gegevens van huurders/gebruikers van de ruimtes, medewerkers en vrijwilligers en andere gevoelige informatie. Denk aan, telefoonnummers, bankrekening- en BSN-nummers, adressen etc. Het kan heel gevoelige en persoonlijke informatie zijn. Wij moeten allemaal incidenten zien te voorkomen en ervoor zorgen dat persoonlijke gegevens of gevoelige informatie niet 'op straat komen te liggen'.

Bewustwording

Om bewustwording waar het gaat om privacy en beveiliging van gegevens door de komst van de AVG bij medewerkers en vrijwilligers wordt hier aandacht aan besteed in de jaarlijkse bijeenkomst voor medewerkers en vrijwilligers. Hiernaast worden medewerkers en vrijwilligers geïnformeerd over de AVG middels een brief eo e-mail.

Rechten van betrokken

Het recht op dataportabiliteit oftewel overdraagbaarheid van persoonsgegevens.
In de AVG (artikel 20) heet dit het 'recht om gegevens over te dragen'. Het houdt in dat mensen het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft. Zo kunnen zij hun gegevens bijvoorbeeld gemakkelijk doorgeven aan een andere leverancier van dezelfde soort dienst. Ook kunnen mensen vragen om gegevens rechtstreeks over te dragen aan een andere organisatie.

Het recht op vergetelheid (artikel 17 AVG), dat wil zeggen dat Siemburg in een aantal gevallen binnen een maand persoonsgegevens moeten wissen als een betrokkene (diegene van wie de organisatie gegevens verwerkt) erom vraagt. Het recht op vergetelheid geldt:

- Wanneer we de gegevens niet meer nodig hebben voor de doeleinden waarvoor we ze verzamelen en verwerken.
- Wanneer we de gegevens niet meer nodig hebben
- Wanneer de betrokkene eerder (uitdrukkelijke) toestemming heeft gegeven aan Siemburg voor het gebruik van zijn gegevens, maar die toestemming nu intrekt.
- Wanneer de betrokkene bezwaar maakt tegen de verwerking.
- Wanneer we de gegevens zonder wettelijk reden verwerken.

We zijn wettelijk verplicht om de gegevens van medewerkers een termijn van 5 jaar te bewaren na uitdiensttreding.

Overzicht verwerkingen

In de AVG hebben we een verantwoordingsplicht, dat wil zeggen dat we kunnen aantonen dat we in overeenstemming met de AVG handelen. De Functionaris voor de Gegevensbescherming (FG is de ICT bestuurder) houdt bij welke persoonsgegevens we verwerken, met welk doel we dit doen, waar deze gegevens vandaan komen en met wie we ze delen. De FG houdt het register van verwerkingsactiviteiten bij. We moeten dit register kunnen verstrekken wanneer de Autoriteit Persoonsgegevens daar om vraagt.
Ook moeten we kunnen laten zien dat we toestemming hebben van de betrokken personen.

Data protection impact assessment (DPIA)

Onder de AVG kunnen we verplicht zijn om een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico’s van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico’s te verkleinen. Dit zou bijvoorbeeld van toepassing kunnen zijn als we een nieuwe technologie zouden gaan gebruiken. De ICT bestuurder in zijn rol als FG zal actie uitzetten om de risico’s van de gegevensverwerking in kaart te brengen.

Privacy by design & privacy by default

Privacy by design houdt in dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat we niet meer gegevens verzamelen dan nodig voor het doel van de verwerking. En dat we de gegevens niet langer bewaren dan nodig.
Privacy by default houdt in dat we technische en organisatorische maatregelen nemen om ervoor te zorgen dat we alléén persoonsgegevens verwerken die noodzakelijk zijn voor het specifieke doel dat we willen bereiken. Dat we niet meer gegevens vragen dan nodig.

Functionaris voor de gegevensbescherming

Als organisatie zijn we verplicht onder AVG om een functionaris Gegevensbescherming aan te wijzen. Van een FG wordt verwacht dat hij of zij bovengemiddelde vakkennis heeft van privacywetgeving en van de praktijk van gegevensbescherming.
De vereiste expertise en vaardigheden omvatten in ieder geval:

- kennis van nationale en Europese privacywet- en regelgeving over gegevensbescherming;
- begrip van de gegevensverwerkingen die de organisatie uitvoert;
- begrip van IT en informatiebeveiliging;
- kennis van de organisatie en de sector waarin die actief is;
- vaardigheden om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.

Meldplicht datalekken

Een informatiebeveiligingsincident kan leiden tot een datalek. Een datalek betekent dat er vertrouwelijke informatie bij een persoon terecht komt, die niet voor hem/haar bedoeld is. De gevolgen kunnen ernstig zijn. Zowel voor degenen om wie het gaat (de betrokkene(n)), als voor Siemburg.

Als er sprake is van een datalek zijn we verplicht om het incident te melden. Het is daarom belangrijk dat je een incident altijd meldt bij de Functionaris Gegevensbescherming (FG), ook als je twijfelt. De FG zal beoordelen of we verplicht zijn om het incident te melden. Tegelijkertijd kunnen we van een incident leren en kan de FG jou helpen en adviseren hoe het incident in het vervolg voorkomen kan worden.
In de AVG dienen we ook de datalekken te documenteren.

SIEMBURG
Stichting Dorpshuis Kruisland

Verwerkersovereenkomsten
Siemburg sluit overeenkomsten met verwerkers, dat zijn samenwerkingspartners die ook persoonsgegevens van medewerkers /vrijwilligers gebruiken.

Hierin worden het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en onze rechten en verplichtingen als verwerkingsverantwoordelijke vastgelegd. Ook bepaalt Siemburg in de verwerkersovereenkomst de instructies voor de verwerking, staat de geheimhoudingsplicht vermeld en bepalingen over beveiliging en subverwerking. De eindverantwoordelijke is de initiatiefnemer van de verwerkersovereenkomst.

Leidende toezichthouder

Voor Siemburg geldt dat de Autoriteit Persoonsgegevens de leidende toezichthouder is als het gaat om de uitvoering van de AVG.

Toestemming

Een aantal van onze gegevensverwerkingen zijn gebaseerd op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming.
Nieuw is dat we moeten kunnen aantonen dat we geldige toestemming van mensen hebben gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo gemakkelijk moet zijn om hun toestemming in te trekken als om die te geven.

Eisen die gesteld worden aan de toestemming zijn:
de toestemming wordt vrijelijk gegeven door de betrokkene, dus zonder druk uit te oefenen;
de toestemming is ondubbelzinnig: er moet sprake zijn van een duidelijke actieve handeling. Bijvoorbeeld een (digitale) schriftelijke of een mondelinge verklaring.

Betrokkenen moeten geïnformeerd zijn over:
1) onze identiteit;
2) het doel van elke verwerking waarvoor we toestemming vragen;
3) welke persoonsgegevens we verzamelen en gebruiken;
4) het recht dat betrokkenen hebben om de toestemming weer in te trekken. we moeten de informatie in een toegankelijke vorm aanbieden. Ook moet deze begrijpelijk zijn zodat iemand een weloverwogen keuze kan maken. Dat betekent dat we duidelijke en eenvoudige taal moeten gebruiken.
de toestemming moet steeds gelden voor een specifieke verwerking en een specifiek doel. Indien we bij de verwerking meerdere doeleinden hebben, dienen we de betrokkene hierover te informeren en betrokkene voor elk doel afzonderlijk toestemming te vragen. Het doel mag niet gaandeweg veranderen.

Tips

Sluit de deur
Bespreek in geen enkel geval vertrouwelijke of persoonlijke informatie in de foyer, op de gang of in een andere openbare ruimte.

Vergrendel je beeldscherm
Vergrendel je (beeld)scherm van je iPad, mobiel of computer zodra je wegloopt van je werkplek. Ook als je even weg bent om bijvoorbeeld koffie te halen, naar de wc gaat. Vaak wordt een scherm na een aantal minuten automatisch vergrendeld, maar laat het hier niet op aankomen en wees pro-actief. Zo voorkomen we dat anderen bij gevoelige informatie kunnen.

Mag ik deze informatie delen?

Om verschillende redenen kunnen anderen jou vragen om gegevens of informatie; via e-mail, internet of telefoon. Stel jezelf de vraag: ‘Mag ik dit delen?’ Als je het niet zeker weet, leg het voor aan de beheerder of de Functionaris Gegevensbescherming.

Verstuur in ieder geval nooit zo maar (persoonlijke of vertrouwelijke) gegevens via whats app, e-mail, internet of telefoon. Zeker niet aan personen, privé-emailadressen en/of instanties die je niet kent. In de meeste gevallen heb je ook eerst toestemming nodig van de betrokkene(n).

Deel ook geen vertrouwelijke informatie bij de kapper, op een verjaardag, thuis of met de buurman. We verwachten dat je hier professioneel en zorgvuldig mee weet om te gaan.

Kijk altijd even achterom

Blijf bij de printer staan terwijl je print en controleer of alles geprint is. Zo voorkom je dat papieren meegenomen of ingekeken kunnen worden.
Zorg dat je vertrouwelijke papieren, mails en documenten met bijvoorbeeld gegevens van een bewoner/cliënt niet per ongeluk ergens laat liggen. Houdt ze bij je of berg ze op in een afgesloten kast. Kijk altijd even achterom voordat je een vergaderruimte of je werkplek verlaat en bij de printer wegloopt. Voorkom dat anderen vertrouwelijke papieren uit de prullenbak kunnen halen. Gebruik een papierversnipperaar of de speciale containers/bakken.

Hou het sociaal

Respecteer iemands privacy. Deel geen vertrouwelijke informatie via publieke (sociale) media, zoals Facebook, Twitter, Linkedin, Whatsapp.

Sluit ramen en deuren, ook van je auto

Sluit ramen en deuren, vanzelfsprekend, zeker aan het einde van de dag? Alleen sluit je ook de (buiten)deur en het raam als je gaat pauzeren of op een hete zomerdag? Ongetwijfeld zijn er veel situaties in de praktijk te benoemen waardoor er een goede reden is dat een raam of deur open staat waar (tijdelijk) geen zicht op is.

Hetzelfde geldt voor je auto. Sluit ook altijd je ramen en deuren van je auto. Vervoer laptops/iPads in de laadruimte van de auto buiten het zicht en laat ze nooit achter in de auto als je de auto parkeert.

Voorkom dat je mobiele telefoon, laptop of iPad gestolen wordt. Laat je (mobiele) apparaten daarom nooit ergens onbeheerd achter. Mocht je je mobiele apparaat kwijt zijn of gestolen? Wacht niet met melden. Informeer zo snel mogelijk de FG.

SIEMBURG
Stichting Dorpshuis Kruisland

Kies een sterk wachtwoord

Het is belangrijk dat we voor iedere website en applicatie een ander wachtwoord gebruiken, één die niet zomaar te raden is én dat we ons wachtwoord voor onszelf houden. Gebruik willekeurige letters, hoofdletters, leestekens en cijfers. Eén die moeilijk te onthouden is. Bijvoorbeeld '1Abo&dDD=8'.
Verder is belangrijk dat je je wachtwoord direct wijzigt als je denkt dat je wachtwoord is uitgelekt.

Schrijf wachtwoorden nooit op, plak ze ook niet op je beeldscherm. Vraagt een website of je je wachtwoord wilt laten onthouden? Klik altijd op 'Nooit' en gebruik overal een ander wachtwoord. Gebruik bijvoorbeeld niet thuis en op je werk hetzelfde wachtwoord en wees altijd alert als iemand (persoonlijk, per mail, telefoon of een website) vraagt om een wachtwoord.

Bewaar informatie op een veilige plek

Om zo veilig mogelijk met gegevens om te gaan, kun je het beste het daarvoor bedoelde programma gebruiken

Bewaar gevoelige informatie altijd in een afsluitbare kast/ruimte. Gebruik geen (eigen) USB-sticks, harde schijven of openbare mappen. De informatie kan misbruikt worden bij o.a. diefstal of verlies.

Print verder zo weinig mogelijk en leg ook geen schaduwadministratie met persoonsgegevens aan voor het geval dat… Overleg met de beheerder of de Functionaris Gegevensbescherming als je in de praktijk ergens tegenaan loopt. Ze kunnen met je meedenken of met je naar een oplossing zoeken. Als je twijfelt of je bijvoorbeeld bepaalde documenten of informatie mag zien, geef het aan. We kunnen van elkaar leren en houden elkaar op deze manier scherp.

Voorkom Phishing

Ontvang je van een onbekende afzender een e-mail, controleer dan o.a. het e-mailadres en gebruik je professionele oordeel. Klik nooit zomaar op een linkje of een bijlage. Ook hiervoor geldt, bij twijfel niet openen of downloaden, maar doorsturen naar je manager of Functionaris Gegevensbescherming.

SIEMBURG
Stichting Dorpshuis Kruisland

E-mails die bedoeld zijn om informatie ´binnen te hengelen´, zoals wachtwoorden, creditcard/-bankgegevens etc., worden ook wel 'phishingmails' genoemd. Ze worden steeds verfijnder, let onder andere op:

- De afzender. Ken je deze persoon? Verwacht je een mailtje van dit bedrijf?
- Controleer het e-mailadres en wat er achter ....@ staat.
- Staat er een linkje in de mail? Klik er niet op, maar ga er met je muis naartoe en kijk of de link die in beeld komt overeenkomt met de link (de tekst in de mail).
- Wees alert als de mail je vertelt dat je iets hebt gewonnen, er nog een factuur open staat of dat je bankpas geblokkeerd wordt etc.