PRIVACY PROTOCOL

Opgesteld door: Kim Voet- van Rumund
Datum: 30-10-2020

AANDACHTSHOUDER GDPR

Er worden 2 aandachtshouders GDPR aangesteld. Deze zien er op toe dat afspraken worden nageleefd en jaarlijks worden geëvalueerd. Dit zijn:

Patricia Raijmakers
Patricia@krachtig-thuis.nl
06-15477419

Laura Peeters
Laura@krachtig-thuis.nl
06-38170987

VERSTUREN INFORMATIE

Voordat informatie over een client wordt verstuurd, wordt hier schriftelijk toestemming voor gevraagd door middel van het formulier 'toestemming delen informatie'. Dit formulier wordt in het digitale dossier op zilliz bewaard.

Privacy gevoelige informatie wordt alleen verstuurd via Zivver, nadat er toestemming is van de client. Berichten met informatie over een client, die per telefoon worden verstuurd, worden via de beveiligde applicatie 'Teams' verstuurd.

VERWERKINGSREGISTER

Krachtig Thuis heeft een verwerkingsregister opgesteld, waarin wordt bijgehouden welke persoonsgegevens worden verwerkt. Deze staat op intranet.

BEWAREN INFORMATIE

Privacy gevoelige informatie wordt alleen bewaard in Zilliz en in het fysieke dossier in een afgesloten kast op het kantoor van Krachtig Thuis (Rossinistraat 9, Oss). Als bestanden bewerkt worden, kunnen ze in een beveiligd sharepoint opgeslagen worden.

BEWAARTERMIJN

Informatie wordt bewaard tot maximaal 20 jaar na het einde van de zorgovereenkomst. Daarna wordt de informatie verwijderd en vernietigd.

TOEGANG PRIVACY GEVOELIGE INFORMATIE

Privacy gevoelige informatie wordt bewaard in het digitale dossier in Zilliz. Alleen medewerkers die direct werken met deze client (Gezinsbegeleider, coördinator, gedragswetenschapper, casusregisseur) en de 2 directeuren van Krachtig Thuis, hebben toegang tot dit digitale dossier.

Wanneer een medewerker zijn dienstverband beëindigd, wordt zijn Zilliz account opgeheven en hij/zij moet de sleutel van het kantoor en de dossierkast inleveren, waardoor hij/zij niet meer bij privacygevoelige informatie kan.

DATA LEK

Een datalek kan vervelende gevolgen hebben voor de personen om wie het gaat. Het is vervelend als bijvoorbeeld namen en adresgegevens, foto's, identiteitsnummers, inloggegevens, salarisgegevens van klanten of medewerkers in onbedoelde handen komen, gewijzigd worden of niet beschikbaar worden gemaakt.

Als zoiets gebeurt moet dat meestal gemeld worden aan de Autoriteit Persoonsgegevens en aan de personen om wie het gaat.

1. ALS MEDEWERKER MELD JE EEN MOGELIJK DATALEK AAN DE PRIVACY OFFICER

Bij een datalek komen persoonsgegevens in onbedoelde handen. Daarbij kunnen de gegevens gewijzigd worden. Ook het niet meer beschikbaar hebben van persoonsgegevens, terwijl dat wel de bedoeling was, is een datalek. Het is niet altijd direct duidelijk of een incident ook een datalek is.
Wat zijn nu mogelijke (signalen van) datalekken:

- Het verliezen van een laptop, smartphone, USB-stick. Ook het verliezen van een geencrypte/versleutelde USB-stick dient intern gemeld te worden!
- Het verliezen van documenten met persoonsgegevens.
- Het ontdekken van persoonsdocumenten (paspoorten e.d.) en personeelsdocumenten op (digitale) plaatsen waar die niet horen.
- Het versturen van een bestand met persoonsgegevens of persoonsdocumenten naar een verkeerd e-mail adres of naar een verkeerd postadres.
- Het versturen van een e-mail met namen in de cc in plaats van bcc als de geadresseerden niets met elkaar te maken hebben.
- Het realiseren dat je waarschijnlijk slachtoffer bent van een phising bericht.

Als je vermoedt dat er een datalek is, meldt dat dan direct aan de aandachtshouder GDPR van je kantoor. En als deze niet aanwezig is (vakantie/ziekte) aan de directeur.

2. WAT MOET DE AANDACHTSHOUDER GDPR DOEN ALS EEN DATALEK ONTDEKT IS

Alle datalekken worden door de privacy officer afgehandeld. Dat moet met spoed gebeuren. Een datalek moet namelijk al binnen 72 uur na ontdekken gemeld worden aan het meldloket van de Autoriteit Persoonsgegevens. Wat moet je als aandachtshouder GDPR doen?

1. IN ONTVANGST NEMEN VAN MELDINGEN EN DEZE VASTLEGGEN IN HET INCIDENTENREGISTER VAN JE KANTOOR.

Zorg dat je bereikbaar bent voor je medewerkers en voor ketenpartners die een datalek melden.
De ketenpartners zijn in ieder geval de verwerkers die een datalek aan jouw kantoor moeten melden.
Zorg dat als je niet bereikbaar bent, je een vervanger hebt, bijvoorbeeld de directeur.
Neem de melding in ontvangst en stel de volgende vragen:

- Wat zijn de gegevens van de melder?
- Wat is er gebeurd?
- In welk systeem staan deze gegevens, welke gegevensdrager bevatten deze gegevens?

Leg de melding vast in het register van incidenten van je kantoor. Dat is een verplicht register.
Vul die melding steeds verder aan als je meer weet.

2. ONDERZOEKEN OF HET EEN DATALEK IS

Stel vast of het een datalek is. Een datalek is het doorbreken van een beveiligingsmaatregel of het gebrek aan een beveiligingsmaatregel waardoor de vertrouwelijkheid, integriteit of beschikbaarheid van persoonsgegevens is geschonden.
Niet ieder incident is een datalek:

- Als je je koffer met slot verliest en je vindt deze weer terug en constateert dat het slot niet geopend is, dan heb je wel een beveiligingsincident, maar de vertrouwelijkheid van de persoonsgegevens in die koffer is niet geschonden.
- Als je een USB-stick verliest en er staan geen persoonsgegevens op, dan heb je wel een beveiligingsincident maar geen datalek.
- Als je vanuit je kantoor een onrechtmatige/illegale gegevensverwerking uitvoert, dan is dat een privacy-incident waar je voor beboet kan worden, maar het is geen datalek.

3. ZO JA, ONDERZOEKEN OF HET EEN MELDENSWAARDIG DATALEK IS

Je moet ieder datalek melden bij de AP, tenzij het lek geen risico's inhoudt voor de rechten en vrijheden van betrokkenen. Dat is een behoorlijk strenge eis, dus je moet een datalek al snel melden aan de AP.
Je moet een datalek ook melden aan jouw klanten als het waarschijnlijk een hoog risico met zich meebrengt voor hun rechten en vrijheden. Vuistregel is dat het dan gaat om bijzondere en/of gevoelige gegevens.
Bijzondere gegevens zijn:

- Gegevens over ras of etnische afkomst;
- Gegevens over politieke opvatting;
- Gegevens over religie of levensbeschouwelijke overtuiging;
- Gegevens over vakbondslidmaatschap;
- Genetische of biometrische gegevens van een individu;
- Gegevens over gezondheid;

- Gegevens over strafrechtelijke veroordeling, strafbare feiten of daarmee verband houdende veiligheidsmaatregelen hebben een vergelijkbare impact als bijzondere gegevens.

Gevoelige gegevens zijn onder meer:
- Inloggegevens en wachtwoorden
- Identiteitsgegevens, bijvoorbeeld paspoort, BSN
- Financiële gegevens van de persoon
- Gegevens waarbij reputatieschade en schaamte kan ontstaan

Melden aan de betrokkenen is niet nodig in de volgende gevallen:
- de gegevens zijn versleuteld, waardoor ze onbegrijpelijk zijn voor onbevoegden;
- je hebt achteraf maatregelen genomen, zoals een remote wipe (wissen van data op afstand, bijvoorbeeld op je mobiele telefoon), om ervoor te zorgen dat het dreigende hoge risico zich waarschijnlijk niet meer zal voordoen;
- de melding zou onevenredige inspanningen vergen. In dat laatste geval moet je echter wel een openbare mededeling doen, bijvoorbeeld op jouw website, zodat de betrokkenen even doeltreffend worden geïnformeerd. En als je volgens de AP ten onrechte hebt besloten om niet te melden aan betrokkenen, dan kan die eisen dat je dat alsnog doet.

In deze situaties moet je nog wel melden aan de AP.

4. INDIEN NODIG, MELDEN AAN DE AUTORITEIT PERSOONSGEGEVENS

Binnen 72 uur na het ontdekken van het datalek moet je de melding doen aan de AP. Dat gaat via een webformulier: https://datalekken.autoriteitpersoonsgegevens.nl

Je kunt eventueel een eerste melding doen die je daarna gaat aanvullen. In de melding aan de AP moet staan:
- de aard van het datalek, inclusief wat voor type betrokkenen en hoeveel betrokkenen en systemen erdoor het lek geraakt zijn;
- de naam en de contactgegevens waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het datalek;
- de maatregelen die je hebt voorgesteld of genomen om het datalek aan te pakken, inclusief eventuele maatregelen om de mogelijke nadelige gevolgen ervan te beperken.

5. ZO NODIG, MELDEN AAN DE BETROKKENEN

Doe de melding aan de betrokkenen. Als het om weinig personen gaat, bel ze op en licht ze in over wat er is gebeurd. Door persoonlijk contact verminder je de reputatieschade. Als het om meer personen gaat doe de melding per email. In de melding aan de betrokkenen moet staan:
- de naam en de contactgegevens waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het datalek;
- de maatregelen die je hebt voorgesteld of genomen om het datalek aan te pakken;
- de eventuele maatregelen die de betrokkene kan nemen om de mogelijke nadelige gevolgen ervan te beperken (bijvoorbeeld wijzigen van wachtwoord).

6. ZO NODIG, TEKST EN UITLEG GEVEN AAN DE AUTORITEIT PERSOONSGEGEVENS

Na de melding kun je mogelijk vragen krijgen van de Autoriteit Persoonsgegevens. Werk daar aan mee.

7. ZO NODIG, TEKST EN UITLEG GEVEN AAN DE BETROKKENEN

Na de melding aan betrokkenen kan het zijn dat je nog extra vragen krijgt van personen die getroffen zijn door het datalek. Geef een eerlijk verhaal en probeer deze personen als klant te behouden.

8. AFSLUITEN VAN INCIDENT

Evalueer wat er is gebeurd. Had je dit incident kunnen voorkomen? Hoe is de afhandeling gegaan? Wat kun je volgende keer beter doen?

3. WAT MOET DE AANDACHTSHOUDER GDPR GEORGANISEERD HEBBEN RONDOM DATALEKKEN?

Als er een datalek is, dan moet er snel en adequaat gehandeld worden. Dat kan alleen als de aandachtshouder GDPR de voorbereiding hierop gedaan heeft. Deze bestaat uit het volgende:

1. Bespreek periodiek met de medewerkers wat mogelijke datalekken kunnen zijn bij jouw kantoor en dat datalekken bij jou moeten worden gemeld.
2. Zorg dat bij alle leveranciers (verwerkers) bekend is dat zij de datalekken bij jou moeten melden.
3. Zorg voor een hulplijn met een security expert die je kan helpen als er een ernstig security incident is.
4. Verzamel enkele documenten om je voor te bereiden op een datalek. Bijvoorbeeld de 'Beleidsregels meldplicht datalek' van de Autoriteit Persoonsgegevens of het boek 'Grip op datalekken' van Kluwer.
5. Zorg voor een hulplijn met een privacy expert die je kan helpen om een datalek te beoordelen.
6. Zorg voor een document waarin je de security incidenten kan vastleggen. Je bent verplicht om een register van (mogelijke) datalekken te hebben.

Ben jij het overzicht kwijt?

Het gevoel dat het allemaal teveel is?

Wordt er aan alle kanten aan je getrokken?

Wij kunnen jou helpen!

Kim Voet-van Rumund & Maartje Wouters

WWW.KRACHTIG-THUIS.NL

06 14 88 00 91 | info@krachtig-thuis.nl