De besloten vennootschap met beperkte aansprakelijkheid ZO!interieurprojecten BV, gevestigd aan het adres Wilhelminastraat 18, 5141 HK Waalwijk, is verantwoordelijk voor de verwerking van persoonsgegevens zoals weergegeven in deze privacyverklaring.

Contactgegevens:

https://www.zointerieursprojecten.nl/

Wilhelminastraat 18, 5141 HK Waalwijk

0416 348 564

info@zointerieurprojecten.nl

Persoonsgegevens die wij verwerken

ZO!interieurprojecten verwerkt uw persoonsgegevens doordat u gebruik maakt van onze diensten en/of omdat u deze zelf aan ons verstrekt.

Hieronder vindt u een overzicht van de persoonsgegevens die wij verwerken:

- Voor- en achternaam
- Geslacht
- Geboortedatum
- Adresgegevens
- Telefoonnummer
- E-mailadres
- Overige persoonsgegevens die u actief aan ons verstrekt in correspondentie of telefonische contacten

Met welk doel en op basis van welke grondslag wij persoonsgegevens verwerken

ZO!interieurprojecten verwerkt uw persoonsgegevens voor de volgende doelen:

- Om onze dienstverlening uit te kunnen voeren;
- U te informeren over wijzigingen van onze diensten en producten;
- Verzenden van onze nieuwsbrief en/of reclamefolder.

Geautomatiseerde besluitvorming

ZO!interieurprojecten neemt niet op basis van geautomatiseerde verwerkingen besluiten over zaken die (aanzienlijke) gevolgen kunnen hebben voor personen. Het gaat hier om besluiten die worden genomen door computerprogramma's of -systemen, zonder dat daar een mens (bijvoorbeeld een medewerker van ZO!interieurprojecten) tussen zit.

Hoe lang we persoonsgegevens bewaren

ZO!interieurprojecten bewaart uw persoonsgegevens niet langer dan strikt nodig is om de doelen te realiseren waarvoor uw gegevens worden verzameld. Uw gegevens worden bewaard gedurende de looptijd van de overeenkomst die ZO!interieurprojecten met u heeft gesloten en gedurende een periode van maximaal twee jaar daarna, tenzij de bewaartermijn op grond van een wettelijke verplichting langer is. In dat geval geldt de wettelijke bewaartermijn.

Verstrekken aan derden

ZO!interieurprojecten verstrekt uw persoonsgegevens niet aan derden, tenzij dit nodig is voor de uitvoering van onze overeenkomst met u of om te voldoen aan een wettelijke verplichting.

Cookies, of vergelijkbare technieken, die wij gebruiken

ZO!interieurprojecten gebruikt alleen technische en functionele cookies en analytische cookies die geen inbreuk maken op uw privacy. Een cookie is een klein tekstbestand dat bij het eerste bezoek aan deze website wordt opgeslagen op uw computer, tablet of smartphone. De cookies die wij gebruiken zijn noodzakelijk voor de technische werking van de website en uw gebruiksgemak. Ze zorgen ervoor dat de website naar behoren werkt en onthouden bijvoorbeeld uw voorkeursinstellingen. Ook kunnen wij hiermee onze website optimaliseren. U kunt zich afmelden voor cookies door uw internetbrowser zo in te stellen dat deze geen cookies meer opslaat. Daarnaast kunt u ook alle informatie die eerder is opgeslagen via de instellingen van uw browser verwijderen.

Hoe wij persoonsgegevens beveiligen

ZO!interieurprojecten neemt de bescherming van uw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als u de indruk heeft dat uw gegevens niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact op met onze klantenservice of via info@zointerieurprojecten.nl

Gegevens inzien, aanpassen of verwijderen

U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast hebt u het recht om uw eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van uw persoonsgegevens door ZO!interieurprojecten en heeft u het recht op gegevensoverdraagbaarheid. Dat betekent dat u bij ons een verzoek kunt indienen om de persoonsgegevens die wij van u opgeslagen hebben in een computerbestand naar u of een andere, door u genoemde organisatie, te sturen.
U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens sturen naar info@zointerieurprojecten.nl
Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan, vragen wij u een kopie van uw identiteitsbewijs met het verzoek mee te sturen. Maak in deze kopie uw pasfoto, MRZ (machine readable zone, de strook met nummers onderaan het paspoort), paspoortnummer en Burgerservicenummer (BSN) zwart. Dit ter bescherming van uw privacy. We reageren zo snel mogelijk, maar in ieder geval binnen vier weken, op uw verzoek.
ZO!interieurprojecten wil u er tevens op wijzen dat u de mogelijkheid heeft om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens. Dat kan via de volgende link: https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteitpersoonsgegevens/tip-ons.

PROTOCOL DATALEKKEN

Melden incident

De meldplicht datalekken geldt voor de gehele organisatie en iedere medewerker. Iedere medewerker die te maken heeft met vermissing/diefstal van zaken die van ZO!interieurprojecten BV of haar opdrachtgevers zijn, of met een informatiebeveiligingsincident, dient dit te melden bij de directie in de persoon van de heer Marcel van Loon. Dit kan telefonisch via 0416 348 564 of via e-mail: marcel@zointerieurprojecten.nl

De melder wordt verzocht zijn/haar naam en contactgegevens te verstrekken, samen met de informatie over het incident. De melder kan namelijk gevraagd worden om aanvullende informatie te geven over het incident. Dit is belangrijk voor de goede en snelle afhandeling van het incident en voor een eventuele melding aan de AP.

Indien de melder twijfelt of er sprake is van een incident of wat hij moet doen, kan hij de directie raadplegen.

Registratie

De directie registreert de incidentmelding. De directie analyseert of er bij het incident persoonsgegevens betrokken zijn. Indien de melding telefonisch is gedaan, vraagt de directie dit na bij de melder.

Nadat telefonisch contact heeft plaatsgevonden, stuurt de melder aanvullend een e-mail met de inhoud van de melding. In die e-mail worden de volgende vragen beantwoord:

1. Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd?

Vermeld hier ook de naam van het betrokken systeem.

2. Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?

Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.

3. Van hoeveel personen zijn de persoonsgegevens betrokken bij het

beveiligingsincident?

Geef a.u.b. een minimum en maximum aantal personen.

4. Omschrijving groep personen om wiens gegevens het gaat.

Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers.

Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.

5. Zijn de contactgegevens van de betrokken personen bekend?

Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?

6. Wat is de oorzaak van het beveiligingsincident?

Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?

7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?

Geef dit a.u.b. zo specifiek mogelijk aan.

Beoordelen of er sprake is van een datalek

Zo snel mogelijk na de melding van een incident beoordeelt de directie of er sprake is van een datalek dat valt onder de meldplicht van de AVG.

De directie stuurt een e-mail met een gemotiveerde beoordeling en een advies van het incident aan de directie. Indien de directie beoordeelt dat het incident geen datalek in de zin van de AVG betreft, dan zorgt de directie ervoor dat de beoordeling schriftelijk wordt teruggekoppeld aan de melder en de directie. Is het incident wel een datalek in de zin van de AVG, dan zal de directie de melding bij de toezichthouder (Autoriteit Persoonsgegevens) doen.

De directie is er verantwoordelijk voor dat het meldingsformulier van de toezichthouder wordt ingevuld en vervolgens wordt toegestuurd aan de toezichthouder. De melding dient door alle betrokken medewerkers direct en met hoogste prioriteit te worden opgepakt.

De directie houdt een register bij waarin alle datalekken die zich voordoen in de organisatie geregistreerd worden. Dit betekent dat ook wanneer een lek niet gemeld hoeft te worden, er een documentatieplicht geldt.

Beslisboom voor de melding aan toezichthouder

Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat alleen een inbreuk hoeft te worden gemeld als deze leidt tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van betrokkenen. Hierbij spelen de volgende factoren een rol:

1) Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals medische/politiegegevens, gegevens over gezondheid, ras of religie of financiële gegevens zijn gelekt.

2) Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.

Er moet in ieder geval gemeld worden als één van onderstaande vragen positief wordt beantwoord.

Zijn gegevens (definitief) verloren gegaan?

Ja melden

Zijn de gegevens bijzonder of zeer omvangrijk?

Ja melden

Zijn de gegevens in onbevoegde handen geraakt?

Ja melden

Aanzienlijk risico op schade aan persoonlijke levenssfeer?

Ja melden

Nee op alle vragen niet melden

Mogelijk is op het moment dat er gemeld moet worden nog geen volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval vindt de melding plaats op basis van de gegevens waarover ZO!interieurprojecten op dat moment beschikt. Eventueel kan de melding naderhand nog worden aangevuld of zelfs worden introkken.

Melden aan betrokkene?

De betrokkene is degene over wie persoonsgegevens worden verwerkt en waarvan de gegevens onderwerp zijn van de datalek. Indien er sprake is van een datalek moet deze aan de betrokkene worden gemeld, als de inbreuk een hoog risico brengt op schade aan diens persoonlijke levenssfeer. Niet in alle gevallen hoeft een datalek aan de betrokkene te worden gemeld.

Voor de beoordeling of aan de betrokkene(n) gemeld moet worden, zijn de volgende vragen van belang.

Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten?

Nee Melden

Zijn de gegevens versleuteld of ontoegankelijk voor degene die geen recht op inzage heeft in deze gegevens?

Nee Melden

Artikel 34(3) van de AVG stelt drie voorwaarden waaronder geen melding aan betrokkenen vereist is. Dit geldt in de volgende situaties:

1. Er zijn technische en organisatorische maatregelen getroffen ter bescherming van de persoonsgegevens vooraf aan het lek. In het bijzonder maatregelen die ervoor zorgen dat de data niet toegankelijk is voor ongeautoriseerde personen. Bijvoorbeeld door encryptie of anonimiseren.
2. Direct na een datalek zijn er acties ondernomen om ervoor te zorgen dat er geen hoog risico meer is op schade aan de persoonlijke levenssfeer van betrokkenen.
3. Het zou van onevenredige moeite zijn om contact op te nemen met individuen, bijvoorbeeld wanneer de contactgegevens van betrokkenen verloren zijn. In dit geval zal er gekozen moeten worden voor een openbare communicatie uiting of een vergelijkbare maatregel.

Termijn van melden

Voor het melden van een datalek aan betrokkenen geldt dat dit ‘onverwijld’ moet gebeuren. Uitgangspunt is dat onnodige vertraging wordt voorkomen, zodat de betrokkene de nodige maatregelen kan treffen. Gelet hierop dient een datalek binnen 72 uur te worden gemeld aan de toezichthouder.

Melden aan andere partijen?

Indien sprake is van samenwerking met andere partijen (ketenverwerking of verwerkers) zal ZO!interieurprojecten moeten beoordelen of een datalek-incident aan de externe partij gemeld moet worden. Dit is geen wettelijke verplichting, maar kan vanuit communicatie redenen raadzaam zijn.

Bij de uitwerking van de communicatiestrategie vindt afstemming plaats welke doelgroepen/ overige partijen worden geïnformeerd over het datalek en op welke wijze.

AFHANDELEN MELDING

De directie houdt een register bij van de meldingen van datalekken. In dit register verwerkt zij de interne en externe meldingen.