

WBP, DOELSTELLINGEN GEGEVENS-GEBRUIK KLOK GROENPROJECTEN

Klok Groenprojecten (hierna te lezen als KGP) maakt gebruik van uw persoonsgegevens conform de wettelijke grondslagen voor de volgende doeleinden:

- KGP verzamelt en gebruikt gegevens die noodzakelijk zijn voor een correcte uitvoering van een overeenkomst, onder andere NAW-gegevens, btw-nummers, rekeningnummers en kenmerken.
- KGP verzamelt en gebruikt NAW-gegevens om een offerte te schrijven nadat u deze hebt aangevraagd.
- KGP verzamelt en gebruikt NAW-gegevens en BSN-nummers van haar werknemers om te kunnen voldoen aan de wettelijke grondslagen van de belastingdienst t.a.v. belastingen en sociale heffingen.
- KGP verzamelt en gebruikt uw NAW-gegevens, e-mail, telefoonnummer voor communicatiedoeleinden, deze gegevens worden niet gebruikt voor het verspreiden van ongeadresseerde/ 'algemene reclame'.

PROCEDURE VAN VERWERKING EN BEVEILIGING.

Uw gegevens komen bij ons binnen via mail, telefonisch of schriftelijk. Deze worden vervolgens naar gelang de vraag verwerkt in bijvoorbeeld een offerte, rapportage of bericht.

Alle gegevens wordt bewaard op de computer of in de archiefkasten op de locatie van KGP, Laarstraat 9a 6654 KJ Afferden. Computers worden beveiligd met behulp van antivirusprogramma's en er wordt gebruik gemaakt van de beveiligde Cloud-service van Microsoft. Op locatie is er 24/7 hondenbewaking aanwezig en de computers zijn met wachtwoord beveiligd.

Gegevens worden bewaard gedurende de wettelijke termijn, wanneer gegevens overbodig zijn worden deze verwijderd(digitaal) of vernietigd(fysiek).

DATALEKPROTOCOL

Dit document beschrijft de verschillende stappen die binnen KGP genomen worden bij een datalek, die valt onder de Meldplicht Datalekken.

VERANTWOORDELIJKHEDEN

Functionaris	Verantwoordelijkheden
Directie	Aannemen en registreren van meldingen van datalekken
Directie	Melden van datalek bij Autoriteit Persoonsgegevens
Directie	Beoordelen en vastleggen van gevolgen en te nemen maatregelen
Directie	Fiatteren van maatregelen
Medewerkers	Melden van datalekken van persoonsgegevens

BESCHRIJVING PROCEDURE

De meldplicht datalekken is een wijziging van de Wet Bescherming Persoonsgegevens en treedt in werking met ingang van 1 januari 2016. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in artikel 13 van WBP. De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking.

Datalekken kunnen ontstaan door:

- o Moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware besmetting);
- o Technisch falen (ICT-storingen);
- o Menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen);
- o Calamiteit (brand datacentrum, wateroverlast);
- o Verloren USB-stick of laptop;
- o Verzenden van email met emailadressen van alle geadresseerden;
- o Het onrechtmatige verwerking van gegevens.

MELDEN BIJ AUTORITEIT PERSOONSgegevens

Een datalek moet onverwijld (binnen 2 dagen) nadat de verantwoordelijke binnen KGP er kennis van heeft genomen, bij de Autoriteit Persoonsgegevens gemeld worden. Het datalek moet ook worden gemeld bij de betrokkenen. In het geval van KGP zijn dit over het algemeen cliënten of medewerkers. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. De betrokkene moet onverwijld in kennis worden gesteld van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer. Een bewerker is verplicht om een datalek te melden bij de verantwoordelijke.

Verantwoordelijke: directeur KGP. De verantwoordelijke heeft zeggenschap over doel en wijze van verwerking. Formeel, juridisch en feitelijk (functioneel) degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Degene die zeggenschap heeft en verantwoordelijk is over doel en middelen van verwerking en beslist over bewaartermijnen, verstrekking inzageverzoeken etc. De verantwoordelijke heeft de regierol (regie over het beheer van privacy in de keten);

Bewerker: degene die de gegevens ten behoeve van de verantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen (ook extern). De bewerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de verantwoordelijke. De bewerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc.

STAPPENPLAN INTERN MELDEN

STAP 1: MELDEN VAN DATALEK

Alle datalekken van persoonsgegevens moeten intern worden gemeld en worden gedocumenteerd door directie. De melding kan door iedere medewerker en iedere bewerker worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van KGP. De melding moet direct en telefonisch worden gedaan bij de directie en schriftelijk worden vastgelegd. Buiten kantoor tijden is de directie bereikbaar.

De directie legt vast:

- Naam van de melder;
- Datum en tijd van de melding;
- Aard van de inbreuk (is er aanmerkelijk risico op verlies of onrechtmatige verwerking?);
- Welke persoonsgegevens vallen onder de melding;
- Om welk aantal en/of gegevensrecords gaat het;
- Welke (groepen) personen zijn betrokken bij de melding;
- Welke maatregelen zijn of worden door de melder getroffen;
- Welke gevolgen zijn er volgens de melder voor de betrokkenen;
- De contactpersoon voor de melding.

STAP 2: INVENTARISEREN GEVOLGEN EN TE NEMEN MAATREGELEN

Na ontvangst van een melding datalek wordt door de directie van KGP beoordeeld en vastgelegd:

De noodzakelijke vervolgacties m.b.t. het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer;

Hetgeen gemeld gaat worden bij de Autoriteit Persoonsgegevens door de <functionaris> (naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records):

De mogelijke gevolgen voor de betrokkenen;

De maatregelen die KGP neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;

De maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;

Contactgegevens voor betrokkenen;

De wijze van afhandeling intern, inclusief communicatie naar melder, betreffende afdeling(-en) en teamleider(s);

Of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad;

Het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit KGP zelf, een bewerker, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregelheden te voorkomen. Indien gewenst vindt overleg plaats met de juridisch adviseur;

Hetgeen intern gecommuniceerd wordt, op welk moment;

Hetgeen extern gecommuniceerd wordt, op welk moment. Er wordt vastgesteld of de pers geïnformeerd moet worden;

Of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd worden;

Op welke wijze er intern wordt gerapporteerd, inclusief actiehouder;

Of eventuele schade is gedekt door de verzekeringspolis.

Eventuele verbeter-/beheersmaatregelen worden vastgelegd in het Verbeterregister.

STAP 3: FIATTERING

De directeur accordeert de uit te voeren activiteiten, zoals vastgesteld, of stelt de uit te voeren activiteiten bij. De door de directeur vastgestelde activiteiten worden uitgevoerd.

STAP 4: MELDING BIJ AUTORITEIT PERSOONSgegevens

De directie meldt binnen 2 dagen het datalek bij de Autoriteit Persoonsgegevens. In ieder geval zal gemeld moeten worden:

- o Aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, aantal gegevensrecords;
- o Beschrijving van de te verwachten gevolgen;
- o Getroffen en/of voorgestelde maatregelen;
- o Informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- o Contactgegevens voor betrokkene;

STAP 5: ONTVANGSTBEVESTIGING AUTORITEIT PERSOONSgegevens

Is er een melding gedaan, dan ontvangt KGP een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal de Autoriteit Persoonsgegevens contact opnemen met KGP om de herkomst van de melding te verifiëren.