1. Inleiding

Dit document beschrijft de verschillende stappen die binnen Jongplus genomen worden bij een datalek, die valt 1.onder de Meldplicht Datalekken.

2. Verantwoordelijkheden

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

3. Beschrijving procedure

De meldplicht datalekken is met een wijziging van de Wet Bescherming Persoonsgegevens (WBP) met ingang van 1 januari 2016 in werking getreden. De komst van nieuwe Europese privacywet, de Algemene verordening gegevensbescherming (AVG) heeft niets aan de meldplicht datalekken veranderd. De AVG stelt wel strengere eisen aan de registratie van de datalekken.

Er is sprake van een datalek wanneer een inbreuk in verband met persoonsgegevens heeft plaatsgevonden (als bedoeld in artikel 4 van de AVG). De persoonsgegevens zijn dan door een inbreuk op de beveiliging verloren gegaan, vernietigd, gewijzigd of op een ongeoorloofde wijze verstrekt of toegang gegeven.

Datalekken kunnen ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen);
- calamiteit (brand datacentrum, wateroverlast);
- verloren USB stick of laptop;
- verzenden van email met emailadressen van alle geadresseerden;
- het onrechtmatige verwerken van gegevens.

3.1 Definities

1. Verwerkingsverantwoordelijke: directeur Jongplus. De verwerkingsverantwoordelijke heeft zeggenschap over doel en wijze van verwerking van persoonsgegevens. 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 et cetera. De verwerkingsverantwoordelijke heeft de regierol (regie over het beheer van privacy in de keten);
2. Verwerker: degene die de persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen (ook extern).

De verwerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de verwerkingsverantwoordelijke. De verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de

opslag van de gegevens et cetera. De verwerker neemt geen andere verwerker in dienst zonder toestemming van de verwerkingsverantwoordelijke. Een verwerker is verplicht om een datalek te melden bij de verwerkingsverantwoordelijke.

3.2 Stappenplan intern melden

3.2.1 Stap 1: Melden van datalek

Alle datalekken van persoonsgegevens moeten binnen 24 uur intern worden gemeld via het *RF Meldingenformulier* en worden gedocumenteerd door de Functionaris Gegevensbescherming. De melding kan door iedere medewerker en iedere verwerker worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van Jongplus De melding moet direct en telefonisch worden gedaan bij de Functionaris Gegevensbescherming en schriftelijk worden vastgelegd. Buiten kantoortijden is de Functionaris Gegevensbescherming bereikbaar.

De Functionaris Gegevensbescherming 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.

3.2.2 Stap 2: Inventariseren gevolgen en te nemen maatregelen

Na ontvangst van een melding datalek wordt door de directie en Functionaris Gegevensbescherming van Jongplus 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 Gegevensbescherming (naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records):

- de mogelijke gevolgen voor de betrokkenen;
- de maatregelen die Jongplus 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 Jongplus zelf, een bewerker, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden 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 (zie PR Preventieve en corrigerende maatregelen).*

3.2.3 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.

3.3 Extern melden

3.3.1 Melden bij Autoriteit persoonsgegevens
Een datalek moet onverwijld (binnen 72 uur) nadat de verwerkingsverantwoordelijke binnen Jongplus er kennis van heeft genomen, bij de Autoriteit Persoonsgegevens gemeld worden.
In ieder geval zal gemeld moeten worden:

- aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, aantal persoonsgegevensregisters;
- beschrijving van de te verwachten gevolgen;
- getroffen en/of voorgestelde maatregelen;
- informatie over te nemen maatregelen door de verwerkingsverantwoordelijke om de nadelige gevolgen te beperken;
- contactgegevens voor betrokkene;

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

3.3.2 Melden bij betrokkene(n)
Het datalek moet ook worden gemeld bij de betrokkene(n). In het geval van Jongplus zijn dit over het algemeen cliënten of medewerkers. Betrokkene is 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.
De melding aan betrokkenen omvat in ieder geval:

- een omschrijving van de aard van de inbreuk;
- de waarschijnlijke gevolgen van de inbreuk;
- de door de verwerkingsverantwoordelijke te nemen of genomen maatregelen om de inbreuk aan te pakken of de eventuele gevolgen van de inbreuk te beperken.
-

3.5 Afwezigheid Functionaris Gegevensbescherming
Bij afwezigheid van de Functionaris Gegevensbescherming (Corine van Mierlo) wordt diens rol ingevuld door de Tweede Functionaris Gegevensbescherming (Wilco Hijink) Als deze ook afwezig is, wordt diens rol ingevuld door de Derde Functionaris Gegevensbescherming (Peter Hijink).

4. Referenties

- PR Klachten en meldingen
- PR Preventieve en corrigerende maatregelen
- RF Meldingenformulier
- RF Verbeterregister