De procedure voor het beheer van datalekken

Glaswerken Wintermans

Om de betrokkenen beter te beschermen, bepaalt het GDPR dat u in geval van verlies, diefstal of lekken van persoonsgegevens, de Gegevensbeschermingsautoriteit (GBA) en/of de betrokkenen **binnen 72 uur na kennisname** van deze veiligheidsinbreuk onmiddellijk op de hoogte moet brengen.

Het belangrijkste moment is dus de kennis van de datalekken.

Als het echter niet waarschijnlijk is dat de inbreuk een risico voor de persoonlijke levenssfeer oplevert, hoeft dit niet altijd te worden gemeld.

o Wie te waarschuwen in geval van datalekken?

- Concreet zijn er drie mogelijke scenario's:

1. **Bewustwording van het datalek via een extern persoon:**

2. **Een persoon die voor het bedrijf werkt, neemt kennis van de informatie:**

3. **Bewustwording van het datalek door een verwerker van het bedrijf:**

Het patroon is dus min of meer terugkerend: een persoon (extern, binnen het bedrijf of onderaannemer) wordt zich bewust van een inbreuk op de persoonsgegevens. Het belangrijkste is dat de informatie snel teruggaat naar het afdelingshoofd, die van zijn kant een e-mail zal opstellen met een bepaalde hoeveelheid informatie die het mogelijk maakt om de schending te identificeren en het risico voor de rechten en vrijheden van de betrokkenen in te schatten.

De DPO komt tussenbeide aan het einde van de informatieketen om te analyseren of het al dan niet nodig is de gegevensbeschermingsautoriteit en/of de betrokkenen op de hoogte te stellen van de overtreding. De DPO zal de verwerkingsverantwoordelijke hierover adviseren en zal de uiteindelijke beslissing nemen.

Hoe moet de gedetailleerde e-mail worden geschreven?

- Onderwerp van de e-mail: GDPR VIOLATION / Naam van de afdeling / Datum van de bevestiging;
- Naam van de persoon die voor het bedrijf werkt en die zich bewust is geworden van de overtreding;
- Omstandigheden van de ontdekking van de overtreding (de gebruikte software, ...) ;
- Het tijdstip (indien mogelijk) waarop de overtreding werd ontdekt;
- De database of de beheerde site die door de overtreding wordt beïnvloed;
- De kwaliteit van het bedrijf met betrekking tot de verwerking (controller, verwerker, ...).

Wat zijn de elementen waarmee rekening moet worden gehouden om de overtreding te karakteriseren?

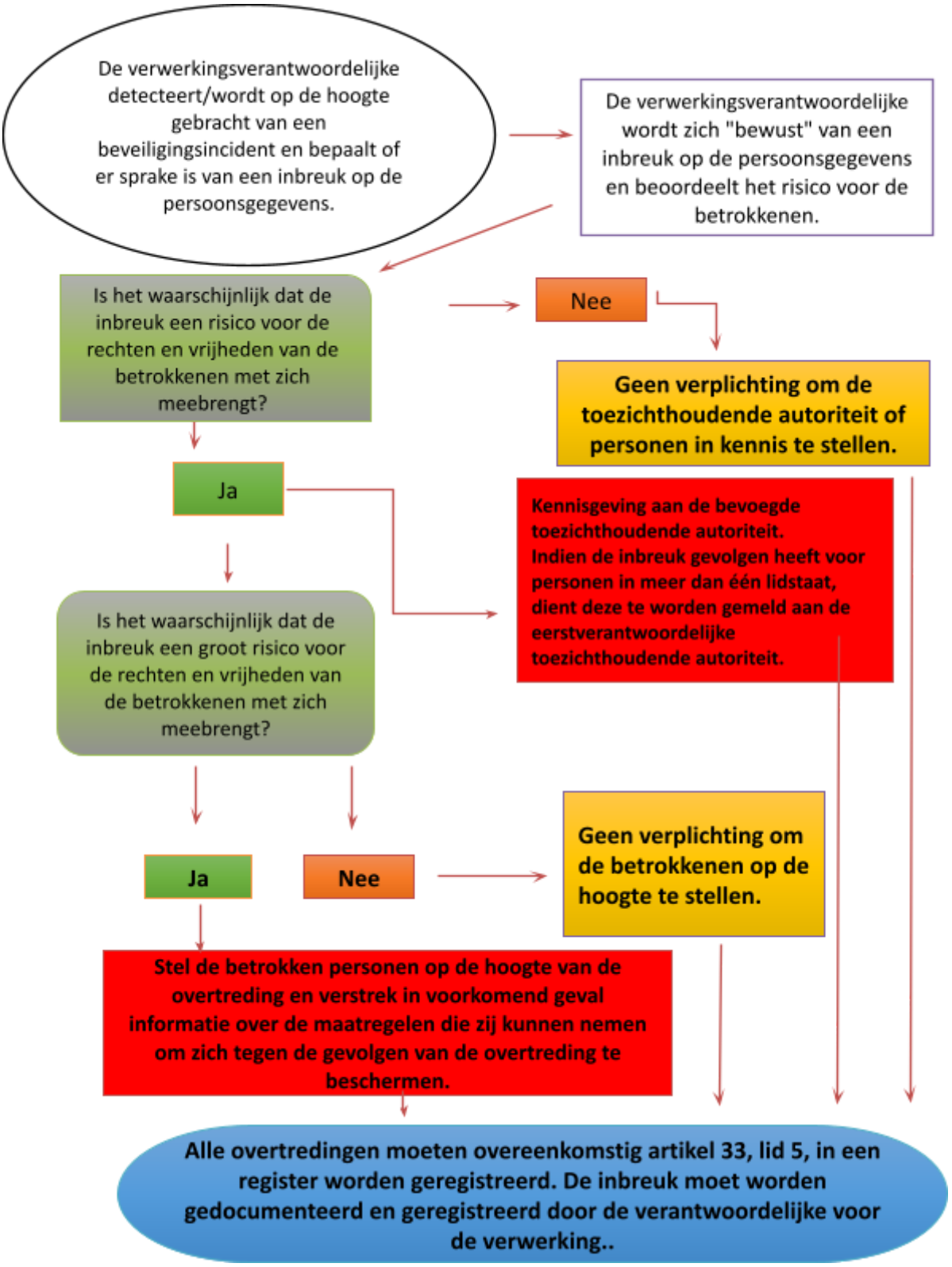
- Beschrijving van de overtreding;
- Datum en tijdstip van ontdekking van de overtreding;
- Soort gegevens waarop de inbreuk betrekking heeft (bankgegevens, medische gegevens, enz.);
- De omvang van de betrokken gegevens;
- Een schatting van het aantal betrokkenen;
- Of de inbreuk al dan niet is gedicht;
- De bestaande beschermingsmaatregelen voor deze gegevens;
- De geografische impact van de gegevensinbreuk;
- De acties die zijn ondernomen om de inbreuk te beheersen;
- De waarschijnlijke gevolgen van de inbreuk;
- De betrokkenheid van een derde of onderaannemer bij de gegevensinbreuk;
- De persoon die verantwoordelijk is voor de database die het slachtoffer is van de inbreuk.

Wat zijn de criteria waarmee rekening moet worden gehouden in de kennisgeving beschikking?

Al deze elementen zullen zorgvuldig moeten worden geanalyseerd om te bepalen of de inbreuk al dan niet een risico inhoudt voor de rechten en vrijheden van de betrokkenen (zie ook het onderstaande schema betreffende de beslisboom).

In ieder geval moet de inbreuk worden gedocumenteerd en bewaard in een daartoe bestemd register.

GBA-besluitvorm voor kennisgeving



Bijvoorbeeld, rekening houdend met alle verzamelde criteria en elementen, zal het niet nodig zijn om de GBA op de hoogte te stellen als: de aard van de activiteiten van de verantwoordelijke voor de verwerking is op zich niet riskant; de omvang van de gegevens en het aantal betrokken personen is verre van significant in vergelijking met de gegevensstromen die PP dagelijks verwerkt; de fraude werd snel geïdentificeerd en tijdig opgelost dankzij de getroffen veiligheidsmaatregelen (het risico bestaat dus niet meer); ondanks de poging om dankzij de veiligheidsmaatregelen toegang tot de gegevens te krijgen, was de toegang tot de gegevens beveiligd; …

Beveiligingsincidentenlogboek

Vul dit register in wanneer u merkt dat er gegevens zijn uitgelekt, of dit nu aan de Gegevensbeschermingsautoriteit of aan de betrokkene moet worden meegedeeld.

Op de volgende pagina vindt u een voorbeeld van een incidentenregister.

Melding van het uitlekken van gegevens aan de gegevensbeschermingsautoriteit

De melding van gegevenslekken bij de Gegevensbeschermingsautoriteit gebeurt via een elektronisch formulier, dat na invulling via een webportaal wordt bezorgd. Let op: formulieren die hen per e-mail worden bezorgd, zullen niet behandeld worden.

Het formulier dient in één van de drie landstalen ingevuld te worden. Technische bijlagen bij het aanvraagformulier mogen naast de drie landstalen ook in het Engels opgesteld zijn (andere talen worden niet aanvaard). Indien niet voldaan wordt aan deze taalvereiste zal de aanvraag als onontvankelijk worden beschouwd.

STAP 1

GA NA OF DE GBA DE BEVOEGDE AUTORITEIT IS

STAP 2

DOWNLOAD HET FORMULIER

STAP 3

VUL HET FORMULIER IN

STAP 4

VERZEND HET FORMULIER VIA DE APPLICATIE

Melding van gegevenslekken

BEVEILIGINGSINCIDENTENLOGBOEK

Verwerkingsverantwoordelijke:

- Naam: Glaswerken Wintermans

- Adres: Lierseweg 326 à 2200 Herentals

- ECB-nummer: 0737.408.153.

Datum van het datalek: ……

□ Beschrijving van het gegevenslek : :

……

……

……..

□ Beschrijving van het gegevenslek :

……

……

……..

□ (indien van toepassing): het gegevenslek is op [datum] gerapporteerd aan :

……

……

……..

Datum van datalek: ……

□ Beschrijving van het gegevenslek : :

……

……

……..

□ Beschrijving van het gegevenslek :

……

……

……..

□ (indien van toepassing): het gegevenslek is op [datum] gerapporteerd aan :

……
……
……