De GDPR in 10 stappen

Stap 10- Voorzie een procedure voor datalekken

De GDPR in 10 Stappen

Stap 10 – Voorzie een procedure voor datalekken

Inleiding

Hoe goed u de GDPR ook naleeft, het kan steeds gebeuren dat u toch een inbreuk vaststelt. Men spreekt dan van een datalek (of gegevenslek). U moet dan ook een procedure uitwerken waarin u beschrijft wat u doet bij zo'n datalek.

Wat is een datalek?

Een datalek of gegevenslek wordt ruim opgevat. Het wordt door de GDPR omschreven als "een inbreuk op de beveiliging van persoonsgegevens die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens".

Het gaat dus bijvoorbeeld om:

- ✓ de onbeschikbaarheid van gegevens, als gevolg van een actie van ransomware ("gijzelen" van gegevens in ruil voor losgeld)
- ✓ het schenden van de integriteit, als gevolg van een ongeoorloofde wijziging van gegevens
- ✓ het schenden van de vertrouwelijkheid van gegevens, als gevolg van het meedelen of ter beschikking stellen van gegevens aan personen die daartoe niet gerechtigd of gemachtigd zijn. Dit kan zowel per ongeluk (een verkeerde manipulatie van gegevens) als onrechtmatig (een gevolg van een computerinbraak) zijn. Hetzelfde geldt voor een medewerker die toegang krijgt tot patiëntengegevens, terwijl hij daar eigenlijk geen toegang mocht toe hebben.

Preventief – richtlijnen om gegevenslekken te vermijden

Elke verwerkingsverantwoordelijke moet ervoor zorgen dat de medewerkers worden gesensibiliseerd om te zorgen voor een voldoende beveiliging. Dit houdt in dat er richtlijnen worden opgesteld en op geregelde tijdstippen aan die richtlijnen wordt herinnerd (zie Stap 8).

Procedure bij gegevenslekken – interne informatie

Medewerkers moeten weten wat er moet gebeuren als er zich een gegevenslek voordoet. Dat houdt met name in dat er wordt aangegeven tot wie (welke dienst of persoon) medewerkers zich moeten richten als ze bepaalde gegevensdragers verliezen, als systemen onbeschikbaar zijn of worden, enz.

Procedure bij gegevenslekken – Crisisteam

Bij grotere partijken wordt er best een soort van "crisisteam" ingesteld. Dit team moet beoordelen of het gegevenslek risico's inhoudt en dus al dan niet moet worden gemeld aan de toezichthouder.
Van dit "crisisteam" maken best deel uit: de bedrijfsleider, de verantwoordelijke van de IT-afdeling of de IT-partner, de persoon die fungeert als aanspreekpunt voor de toezichthouder.

Inventaris van gegevenslekken

De GDPR bevat de verplichting om alle inbreuken in verband met persoonsgegevens te documenteren. Dit komt neer op het opmaken van een inventaris van alle gegevenslekken, ongeacht het risico dat eraan verbonden is. Op die manier kan de toezichthoudende autoriteit, bij een latere controle, nagaan of de verantwoordelijke de verplichting tot het melden en meedelen van lekken wel op een correcte manier toepast.

Zo'n inventaris moet ook de gegevenslekken vermelden die niet leiden tot een risico en dus niet aan de toezichthouder gemeld of aan de betrokkene meegedeeld moeten worden. Dat maakt het tot een zware, vooral administratieve verplichting.

Melding aan de Gegevensbeschermingsautoriteit en de betrokkene

Bij elk gegevenslek moet u analyseren of het lek een risico inhoudt voor de rechten en vrijheden van de betrokkenen. Is dat niet het geval, dan volstaat een melding in uw interne inventaris.
Is er wel een risico, dan moet u het gegevenslek binnen de 72 uur melden aan de Gegevensbeschermingsautoriteit via een speciaal formulier dat u terugvindt op https://www.gegevensbeschermingsautoriteit.be/melding-gegevenslekken-algemeen.

Houdt het gegevens lek een *hoog risico* in voor de rechten en vrijheden van de betrokkenen, dan moet u dit lek tevens onmiddellijk aan de betrokkene zelf melden.

Checklist

- ❑ Ik heb een procedure opgesteld voor datalekken.
- ❑ Ik heb mijn medewerkers ingelicht over deze procedure en over preventieve maatregelen.
- ❑ Ik heb een inventaris van eventuele gegevenslekken.

Procedure bij Datalekken + Model van logboek

Procedure

Stap 1: Analyseer of de inbreuk wel degelijk 'persoonsgegevens' betreft, en zo ja, of u verantwoordelijk bent voor de verwerking van die persoonsgegevens.

Stap 2: analyseer de omvang van het datalek:

- Over hoeveel gegevens gaat het?
- Over hoeveel personen gaat het?
- Werden gevoelige gegevens gelekt?
- Werden gegevens gelekt over kwetsbare groepen?

Stap 3: Analyseer of de inbreuk een risico inhoudt voor de rechten en vrijheden van de natuurlijke personen over wie de gegevens gaan.

> Bijvoorbeeld: Als u per ongeluk een mail verstuurt met een persoonsgegeven een collega, die eigenlijk die mail niet moest krijgen, is dat technisch gezien een inbreuk. Omdat het gaat om een collega en slechts één persoonsgegeven is het risico van deze inbreuk voor de betrokken echter zeer beperkt. Moest daarentegen per ongeluk een selectie van uw klantenbestand openbaar worden, is dat wel een hoog risico voor de betrokkenen.

Stap 4: Is er geen risico voor de rechten van de betrokken?

> Dan volstaat het de inbreuk op te lijsten in het logboek hieronder. Op basis van dat logboek kan u dan op termijn bekijken of er hier of daar extra beveiligingsmaatregelen nodig zijn.

Stap 5: Is er wel een risico voor de rechten van de betrokkene, dan moet u dit melden aan de Gegevensbeschermingsautoriteit (binnen de 72 uur) en de betrokke(n) (onmiddellijk).

a. Met vermelding van :
    i. De aard van de inbreuk
    ii. De categorieën van betrokkenen en persoonsgegevens, en bij benadering het aantal van beiden
    iii. Naam en contactgegevens waar de Gegevensautoriteit u kan bereiken voor meer informatie
    iv. De waarschijnlijke gevolgen van de inbreuk
    v. De maatregelen die u voorstelt of reeds heeft genomen om de inbreuk aan te pakken, en de gevolgen te beperken.
b. De melding aan de Gegevensbeschermingsautoriteit gebeurt via een specifiek formulier dat u terugvindt op hun website: https://www.gegevensbeschermingsautoriteit.be/melding-gegevenslekken-algemeen

Logboek datalekken

Vul dit register in telkens u een datalek vaststelt, ongeacht of dit moet gemeld worden aan de Gegevensbeschermingsautoriteit of aan de betrokkene.

Verwerkingsverantwoordelijke:

- **Naam: …**
- **Adres: …**
- **KBO-nummer:…**

❑ **Datum van het Datalek:** ……

☐ Beschrijving van het datalek: :

……

……

☐ Maatregelen om een lek in de toekomst te vermijden: :

……

……

☐ (indien van toepassing): het datalek werd op [*datum]* gemeld aan:

……

……

❑ **Datum van het Datalek:** ……

☐ Beschrijving van het datalek:

……

……

☐ Maatregelen om een lek in de toekomst te vermijden: :

……

……

☐ (indien van toepassing): het datalek werd op [*datum]* gemeld aan:

……

……

❑ **Datum van het Datalek:** ……

☐ Beschrijving van het datalek: :

……

……

☐ Maatregelen om een lek in de toekomst te vermijden: :

……

……

☐ (indien van toepassing): het datalek werd op [*datum]* gemeld aan:

……

……