Protocol AVG

1 Doel

Voor organisaties die persoonsgegevens verwerken is een meldplicht voor datalekken van toepassing. Onder de Algemene verordening Gegevensbescherming (AVG) moet iedere inbreuk in verband met persoonsgegevens worden gemeld bij de toezichthouder, de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat deze een risico inhoudt. Dit houdt in de praktijk in dat organisaties die een ernstig datalek hebben, dit direct moeten melden. In sommige gevallen moet dit ook gemeld worden aan de mensen van wie de persoonsgegevens zijn gelekt.
Dit document beschrijft de werkwijzen binnen Amarant Groep bij het signaleren van een (mogelijk) datalek en hoe dit vervolgens te registreren, te beoordelen en, waar nodig, te melden.

2 Toepassingsgebied

Deze procedure heeft betrekking op alle medewerkers en inhuurkrachten die werkzaam zijn bij of voor ‘t Opstapje, op verwerkers van persoonsgegevens en op ketenpartners die met ons samenwerken en daarbij gebruik maken van persoonsgegevens van onze organisatie.

3 Definities en afkortingen

In dit reglement worden de begrippen uit de Algemene Verordening Gegevensbescherming (AVG/GDPR) ongewijzigd gebruikt.

4 Procedure

4.1 Signaleren en intern melden

Er is sprake van een datalek als er een inbreuk plaatsvindt op de beveiliging van persoonsgegevens. Dat is bijvoorbeeld het geval wanneer onbedoeld toegang wordt geboden tot persoonsgegevens of als sprake is van vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie. Niet alleen het vrijkomen of lekken van gegevens resulteert in een datalek, ook wanneer onrechtmatig gegevens worden verwerkt is hiervan sprake. Om een voorval te kunnen kwalificeren als een datalek, moet sprake zijn van een daadwerkelijk beveiligingsincident. Dit is het geval bij inbraak in een databestand (hacken), maar ook een kwijtgeraakte usb-stick, een gestolen laptop, een laptop die in de trein is blijven liggen of een brand in een datacentrum zijn datalekken.
Voorbeelden van datalekken zijn, onder andere:

- Kwijtgeraakte USB-stick met medewerker- en cliëntgegevens;
- Gestolen laptop met medewerker- en cliëntgegevens;
- Kwijtgeraakte smartphone met e-mail inhoud en bijlagen;
- Delen van gegevens zonder toestemming of zonder duidelijke wettelijke grondslag;
- Inbraak in databestanden of systemen door een hacker;
- Beeldschermen die bekeken zijn of kunnen worden door derden;
- Het verzenden van een externe e-mail met persoonsgegevens aan een verkeerd geadresseerde,
- Een mail aan externen waarbij de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden (geen BCC gebruikt);
- Het achterblijven van documenten met persoonsgegevens op printers, scanners en of kopieerapparaten.

Onmiddellijk nadat een werknemer heeft ontdekt of anderszins heeft gemerkt dat sprake kan zijn van verlies of onrechtmatige verwerking van persoonsgegevens zoals hierboven beschreven, moet dit gemeld worden. Melden doe je direct bij de directeur.

4.2 Analyseer impact datalek
De directeur stelt samen met de melder of met experts (bijvoorbeeld applicatie- of systeemspecialisten) eerst vast of het lek nog voortduurt, welke actie genomen moet worden om het lek te stoppen of verdere schade te voorkomen en voert deze acties uit of laat ze uitvoeren.
Daarna onderzoekt de directeur, samen met de melder, op wie de persoonsgegevens betrekking hebben (cliënten, medewerkers of anders), welke persoonsgegevens eventueel zijn gelekt (adresgegevens, contactgegevens, gegevens over de gezondheid of andere gevoelige gegevens) en hoeveel persoonsgegevens bij het incident betrokken zijn.
De directeur neemt al deze informatie op in de registratie ('call') en vult aan met relevante informatie tijdens het verdere verloop van het proces.

4.3 Meld datalek aan AP
Wanneer duidelijk is wat de omvang van het lek is en welke persoonsgegevens erbij betrokken zijn;
Als er geen bijzondere persoonsgegevens zijn gelekt, bepalen zij op basis van de aard en de omvang van het datalek of er gemeld gaat worden aan de AP.
Indien er sprake is van een datalek waarbij 'gevoelige gegevens' zijn gelekt (o.a. bijzondere persoonsgegevens, financiële gegevens, wachtwoord/inlognaam combinatie) zal in ieder geval gemeld moeten worden.
Wanneer vaststaat dat er een meldenswaardig datalek heeft plaatsgevonden ('t Opstapje heeft een beperkte tijd om onderzoek te doen naar aard en omvang van het datalek[1]) zal de directeur, binnen 72 uur nadat kennis is genomen van het datalek, melding aan de AP doen. Melding moet worden gedaan met behulp van het meldingsformulier op de site van de AP. Een melding kan worden teruggetrokken als blijkt dat er geen sprake was van een meldenswaardig datalek of worden aangevuld als er aanvullende informatie beschikbaar komt.

4.4 Meld datalek aan betrokkenen
Een melding aan de AP moet altijd plaatsvinden als een van de omstandigheden zoals beschreven in de vorige paragraaf zich voordoet. Een melding aan de betrokkene dient vervolgens plaats te vinden als het datalek voor hun een hoog risico inhoudt. Dit betekent dat, naast de overwegingen om te melden aan de AP, er door de directeur een daadwerkelijke nieuwe afweging gemaakt moet worden voor melding aan de betrokkene. In tijd kunnen en mogen deze overwegingen uiteraard gelijktijdig plaatsvinden.
Melding aan betrokkene(n) kan in ieder geval achterwege blijven indien:
1. er sprake is van goede versleuteling (encryptie) van de verloren persoonsgegevens;
2. dit onevenredig veel inspanning kost. In dat geval kan worden volstaan met een openbare mededeling;
3. de verwerkingsverantwoordelijke achteraf maatregelen heeft genomen om te zorgen dat het hoge risico zich waarschijnlijk niet meer voor zal doen.

Wanneer melding aan betrokkenen noodzakelijk is, zal de informatie in ieder geval bestaan uit:
1. de aard van de inbreuk;
2. de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen (contactgegevens);
3. de maatregelen die zijn aanbevolen om de negatieve gevolgen van de inbreuk te beperken.

4.5 Meld datalek aan overige partijen
Het gevaar is aanwezig dat de communicatie over een datalek wordt overgenomen door andere partijen/platforms zoals lokale, landelijke of sociale media, eigen medewerkers of ketenpartners waardoor als gevolg van ruis in de communicatie een datalek alsnog onnodig kan escaleren.
Indien communicatie naar derden (externen, media/pers e.d.) noodzakelijk is, gelden de afspraken uit het protocol "crisismanagement en –communicatie".

4.6 Evalueer, rapporteer en documenteer
Tijdens en na de afwikkeling van een incident en eventuele melding, wordt alle documentatie verzameld en toegevoegd aan de call. Documentatie kan bestaan uit bespreekverslagen, ingevulde checklist, printscreens, e-mails, controle op logging, bevindingen van ICT-specialisten of experts, processen-verbaal en de (uitwerking/uitvoering van de) communicatiestrategie.
De directeur voert een evaluatie uit en rapporteert waar nodig. Indien noodzakelijk wordt dit protocol aangepast en worden lessons-learned teruggekoppeld aan de organisatie.

5 Bijlage 1: weergave flow melding datalek

Invoegen stroom diagram

6 Bijlage 2: Onderzoeken/analyseren incident (BOB; beeldvorming, oordeelsvorming, besluitvorming)

1. Wat is er precies met de gegevens gebeurd?
2. Wat is de aard van de getroffen gegevens?
a. Bijzondere gegevens: godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap vakbond en strafrechtelijke gegevens
b. Gegevens van gevoelige aard:
i. Financieel of economisch (schulden),
ii. Stigmatiserend (verslaving, naaktfoto's, specifieke problemen),
iii. inloggegevens, gegevens die bruikbaar zijn voor identiteitsfraude (kopie ID, BSN, handtekening, biometrische gegevens),
iv. gegevens die vallen onder beroepsgeheim.
3. Wat is de omvang van het incident?
a. Aantal getroffen personen.
b. Hoeveelheid gegevens per getroffen persoon.
c. Worden de getroffen gegevens binnen een keten gedeeld?
4. Wat is de impact op de betrokkenen?
a. Is sprake van kwetsbare groepen (kinderen, zieken, verstandelijk beperkten, bedreigde personen)?
b. Is er kans op financieel nadeel?
5. Repareren van de inbreuk.
a. Maatregelen treffen om de gevolgen van het incident te beperken.
b. Voorkomen van soortgelijke incidenten in de toekomst.

Meldplicht AP: indien sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.
1. Zelf afwegen aan de hand van de aard van de gegevens, de omvang van het incident en de impact op de betrokkenen.
2. 'Onverwijld' en binnen 72 uur, daarna kan de melding evt. aangevuld of ingetrokken worden.

Doelstelling is om betrokkenen altijd te informeren. In ieder geval informeren als de inbreuk op de beveiliging waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer.
1. Alleen in geval van ook meldplicht AP.
2. Informeren hoeft niet indien de getroffen persoonsgegevens onbegrijpelijk of ontoegankelijk zijn gemaakt (versleuteling of remote wissen).
a. Bij vernietiging (geen back-up) of aantasting (wijziging) van gegevens helpen deze beschermingsmaatregelen niet.
b. Alle persoonsgegevens moeten zijn versleuteld op moment van de inbreuk. De versleuteling moet adequaat zijn.
c. Afweging ongunstige gevolgen persoonlijke levenssfeer.
i. Kan betrokkene last krijgen van de inbreuk, materiële of immateriële schade lijden (aard gegevens, impact, kwetsbare groep)?
ii. Kan betrokkene zichzelf beter beschermen als hij de inbreuk kent?
3. Bij zwaarwegende belangen kan informatie aan betrokkenen achterwege blijven.
4. AP kan alsnog verlangen dat betrokkenen worden geïnformeerd.
5. De informatie moet betrokkenen in staat stellen om de inbreuk op hun persoonlijke levenssfeer zoveel mogelijk te beperken.