Protocol datalekken voor Fidé Hypotheken & Verzekeringen

In dit protocol is de Algemene Verordening Gegevensbescherming (AVG) EU 2016/679 als uitgangspunt genomen, omdat deze geacht wordt vóór 25 mei 2018 te zijn ingevoerd. In de AVG is het begrip “datalek” niet bekend en wordt dit incident een “inbreuk in verband met persoonsgegevens” genoemd; vanwege de bekendheid van het woord ”datalek” zullen we in dit protocol dit begrip echter meestal hanteren.

Enkele relevante definities en (delen uit) artikelen van de AVG:

Definitie AVG art. 4 lid 1: Persoonsgegevens: “alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.”
Er is dus sprake van “persoonsgegevens” als die alleen of in samenhang met elkaar kunnen leiden tot identificatie van een levend individu. De AVG is van toepassing als de persoonsgegevens in een bestand zijn opgenomen en als het gegevens betreffen van een zich in de EU bevindende persoon, ongeacht of de verwerking in de EU plaatsheeft. De AVG gaat dus niet over data die niet tot identificatie van een levend individu kunnen leiden.

Definitie AVG art. 4 lid 12: Een inbreuk in verband met persoonsgegevens (datalek) is “een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.”
In feite is er dus sprake van een datalek als persoonsgegevens zich door onvoldoende beveiliging bevinden op een plek waar ze niet thuishoren.

Organisaties in de EU zijn door de AVG gehouden om (art. 32 e.v.) “rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico’s voor de rechten en vrijheden van personen technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen”.
Dus vanuit het algemeen behoorlijkheidsbeginsel (art. 5 lid1) en het integriteitsbeginsel (art. 5 lid 2 sub f) is het essentieel dat de verwerkingsverantwoordelijke (maar ook de verwerker indien van toepassing) technische en organisatorische beveiligingsmaatregelen neemt ter beveiliging van de aan haar toevertrouwde persoonsgegevens. Aanvullend is de plicht om de toezichthouder (i.c. in Nederland de Autoriteit Persoonsgegevens (AP)) te informeren over inbreuken op de beveiliging (art. 33) en onder omstandigheden ook de betrokkenen (art. 34).

Fidé Hypotheken & Verzekeringen is een zakelijke dienstverlener die bemiddelt en adviseert over bank-en kredietwezen, verzekeringen, vermogen.
Fidé Hypotheken & Verzekeringen. is een financiële instelling waarop de Wet op het financieel toezicht (Wft) van toepassing is. Omdat deze wet op een aantal aspecten prevaleert boven de AVG is voor Fidé Hypotheken & Verzekeringen in een voorkomend geval de verplichting om een datalek te

melden aan betrokkene(-n) niet van toepassing vanuit de Wbp of AVG. De verplichting om aan betrokkene(-n) te melden komt dan voort uit de zorgplicht die Fidé Hypotheken & Verzekeringen. als financiële onderneming heeft. Voor dit protocol hanteren we echter de criteria uit de AVG aangaande meldplicht van datalekken.

Voor dit protocol wordt ervan uitgegaan dat Fidé Hypotheken & Verzekeringen als entiteit (overwegend) de rol van "verwerker" heeft omdat deze meestal niet het doel en de middelen (om dat doel te bereiken) bepaalt voor de verwerking van persoonsgegevens. Mogelijk kent Fidé Hypotheken & Verzekeringen bij sommige verwerkingen de rol van "verantwoordelijke" zoals in de eigen personeelsadministratie. Het stappenplan in dit protocol verandert daardoor niet, alleen geldt de meldplicht dan in die situatie aan de "verwerkingsverantwoordelijke" in plaats van aan de Autoriteit Persoonsgegevens.

De melding van een datalek is omschreven in artikel 33 van de AVG. Samengevat verlangt de tekst van deze verordening dat verwerkingsverantwoordelijken een datalek zonder onnodige vertraging en indien mogelijk binnen 72 uur na constatering van de inbreuk melden bij de Autoriteit Persoonsgegevens tenzij "het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen". In de rol van verwerker zal Fidé Hypotheken & Verzekeringen zonder onredelijke vertraging de verantwoordelijke op de hoogte stellen van de inbreuk met vermelding van de aard van de inbreuk, de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en bij benadering het aantal betrokkenen en persoonsgegevensregisters in kwestie.
Hoewel datalekken altijd vermeld dienen te worden in het privacy-dossier, kan een melding aan de AP of aan de verwerkingsverantwoordelijke achterwege blijven als de inbreuk redelijkerwijs geen risico voor betrokkene(-n) inhoudt.

De melding aan de AP gebeurt via de link
https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
die leidt naar het meldloket datalekken.
Art. 34 van de AVG luidt: "Indien de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkenen de inbreuk in verband met persoonsgegevens onverwijld mee." Voorbeelden van een hoog risico zijn het verlies van controle over hun persoonsgegevens waardoor identiteitsfraude tot de mogelijkheden behoort, het niet kunnen uitoefenen van hun rechten, kans op discriminatie, financiële verliezen en reputatieschade.

De volgende rollen binnen Fidé Hypotheken & Verzekeringen worden onderscheiden:

- **IT-verantwoordelijke.** Deze functionaris heeft geen bevoegdheden vooraf en ontvangt zo snel mogelijk na constatering van de inbreuk instructies van de bestuurder over hoe te handelen.
- **Bestuurder.** Deze functionaris is bestuurder van Fidé Hypotheken & Verzekeringen en is eindverantwoordelijke voor de AVG en de AP en ontvangt zonder onnodige vertraging alle relevante informatie omtrent (mogelijke) datalekken van medewerkers, derden en/of verwerkers.

De volgende opeenvolgende stappen zijn in het proces van omgaan met een (mogelijk) datalek van toepassing en worden hierna per stap toegelicht:

1) Ontdekking van een mogelijke inbreuk.
2) Interne melding van de mogelijke inbreuk.
3) Beoordeling van de ernst van de gemelde inbreuk, zowel voor Fidé Hypotheken & Verzekeringen als voor de betrokkene(-n).
4) Response door de IT verantwoordelijke en indien nodig bestrijding van het lek.
5) Response door de privacy-officer en indien nodig melding van de inbreuk aan AP.
6) Response door de privacy-officer en indien nodig melding van de inbreuk aan de betrokkene(-n).
7) Bepaling van de acties voor verbetering van de beveiliging, zowel technisch als organisatorisch.
8) Regelen van de nazorg aan de betrokkene(-n).
9) Registreren, evalueren en verbeteren.

Ontdekking van een mogelijke inbreuk en interne melding.
Fidé Hypotheken & Verzekeringen instrueert haar medewerkers dat ALLE signalen die kunnen wijzen op een datalek gemeld dienen te worden aan de bestuurder.

Beoordeling van de ernst van de gemelde inbreuk.
De bestuurder gaat in overleg met de melder van het incident en bouwt zich daarmee een beeld op van het betreffende incident aan de hand van de volgende vragen:

- Waar heeft het incident plaatsgevonden?
- Welke systemen zijn daarbij betrokken?
- Indien van toepassing: waar heeft het verlies of de diefstal van fysieke gegevensdragers plaatsgevonden en onder welke omstandigheden?
- Om welke data handelt het? (AVG meldplicht is alleen van toepassing op persoonsgegevens)
- Om welke persoonsgegevens gaat het en om hoeveel personen?
- Is er mogelijk sprake van schending van vertrouwelijkheid, beschikbaarheid en/of van integriteit van de persoonsgegevens?
- Welke bedrijfsprocessen kunnen verstoord raken door het incident?
- Wat is de vermoedelijke oorzaak.
- Is het datalek voorbij of is de verwachting dat het systeem verder geïnfiltreerd kan worden?

Response door de IT verantwoordelijke en bestrijding van het lek.
De IT verantwoordelijke is niet bevoegd behoudens opdrachten ten tijde van of direct na het ontstaan van het lek door bestuurder. De bestuurder kan de IT-verantwoordelijke o.a. het volgende opdragen uit te voeren om de inbreuk te bestrijden of te mitigeren.

- Tijdelijk blokkeren van accounts
- Aanpassen van de firewall configuraties
- Wijzigen van wachtwoorden
- Verzamelen van bewijsmateriaal om de veroorzaker aan te kunnen wijzen en aan te kunnen blokkeren
- Op afstand wissen van bestanden op geïnfecteerde devices.
- Dit zijn slechts voorbeelden van mogelijk te nemen maatregelen.

Response door de bestuurder en indien nodig melding van de inbreuk aan de AP.

Indien de conclusie uit de beoordeling van de ernst van de gemelde inbreuk is dat er waarschijnlijk sprake is van een risico voor de rechten en vrijheden van de betrokkene(-n) doet de bestuurder binnen 72 uur na constatering van de inbreuk melding hiervan aan de AP via de link https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
Hieronder verschijnt een pagina met de button “nieuwe melding” waarna een vragenlijst volgt die geheel beantwoord dient te worden door de bestuurder. Indien hij of zij dat nodig of gewenst acht, kan de bestuurder advies over de te geven antwoorden inroepen van een externe deskundige.

Response door de bestuurder en indien nodig melding van de inbreuk aan de betrokkene(-n).
Bij een hoog risico voor de betrokkene(-n) dienen deze van de inbreuk op de hoogte te worden gesteld. De bestuurder bepaalt de hoogte van het risico door een inschatting te maken van de kans op nadelige gevolgen voor de betrokkene(-n) en de mate van ernst voor de gevolgen van de inbreuk voor de betrokkene(-n). De bestuurder bepaalt welke vorm van communicatie met de betrokkene(-n) het meest geschikt is om de schade voor de betrokkene(-n) zoveel mogelijk te beperken. De mededeling aan betrokkene(-n) bevat tenminste

- een omschrijving van het feit in duidelijke en eenvoudige taal
- de naam en contactgegevens van de bestuurder
- de waarschijnlijke gevolgen van de inbreuk
- de maatregelen die Fidé Hypotheken & Verzekeringen genomen heeft om de nadelige gevolgen voor de betrokkene(-n) te beperken
- de maatregelen die de betrokkene(-n) zelf moet(-en) nemen om die gevolgen te beperken en herhaling te voorkomen.

Bepaling van de acties voor verbetering van de beveiliging, zowel technisch als organisatorisch.
Datalekken zijn bijna altijd een gevolg van onvoldoende beveiliging van de gegevens op een bepaald moment. Fidé Hypotheken & Verzekeringen tracht steeds te voldoen aan een adequate beveiliging conform artikel 32 van de AVG waarin sprake is van “passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen” zulks “rekening houdend met de stand van de techniek en de uitvoeringskosten” en het risico voor de betrokkene(-n). Dit betekent een vergaande inspanningsverplichting om de beveiligingsmaatregelen op een passend niveau te brengen. Bij de bepaling van de acties voor verbetering houdt de IT verantwoordelijke onder meer rekening met:

- mogelijkheden voor pseudonimisering en encryptie van persoonsgegevens
- de mogelijkheden om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en de veerkracht van de verwerkingssystemen te garanderen
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid en de toegang tot de persoonsgegevens tijdig te herstellen (PDCA cyclus)
- een procedure om voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de genomen maatregelen
- regelmatige scholing en instructie van personeel vanFidé Hypotheken & Verzekeringen waardoor datalekken door menselijk falen tot een minimum worden teruggebracht.

Regelen van de nazorg aan de betrokkene(-n).
Rekening houdend met de ernst van de gevolgen van de inbreuk voor de betrokkene(-n) bepaalt de bestuurder welke additionele acties gewenst zijn om het eventueel geschonden vertrouwen in Fidé Hypotheken & Verzekeringen te herstellen en de reputatieschade voor Fidé Hypotheken & Verzekeringen te beperken.

Registreren, evalueren en verbeteren.
De bestuurder registreert elk incident, ook als dit geen datalek blijkt te zijn en dus niet gemeld hoeft te worden. Deze registratie stelt Fidé Hypotheken & Verzekeringen in staat om structureel aan verbetering te werken. De registratie vindt plaats in een daarvoor gereserveerd hoofdstuk in het privacy-dossier vanFidé Hypotheken & Verzekeringen.
De bestuurder evalueert op jaarbasis de geregistreerde incidenten en neemt maatregelen voor verbetering.
Voor wijzigingen in de zienswijze, voor richtsnoeren, publicaties en voor toelichtingen op het melden van datalekken volgt de privacy-officer de meldingen van de Autoriteit Persoonsgegevens middels publicaties op hun site www.autoriteitpersoonsgegevens.nl en middels een abonnement op de nieuwsbrief van deze autoriteit.

Onderstaand een schematische voorstelling voor instructiedoeleinden van de melding op grond van de huidige Wet bescherming persoonsgegevens (Wbp):