DATALEKKEN BELEID EN PROCEDURE

1. INLEIDING

AANNEMINGSMAATSCHAPPIJ CFE NV en haar dochtervennootschappen (hierna de “Vennootschap”) hecht veel belang aan de bescherming van persoonsgegevens en aan de bescherming van vertrouwelijke informatie. De Vennootschap neemt haar verplichtingen in het kader van de Algemene Verordening Gegevensbescherming dan ook ernstig.

Als werkgever dringen we er bij al onze medewerkers die in contact komen met persoonsgegevens en vertrouwelijke informatie op aan hier zeer zorgvuldig mee om te gaan.

Deze Policy is van toepassing op iedereen die op welke manier ook, tijdens de uitoefening van zijn/haar functie in contact komt met vertrouwelijke informatie (zakengeheimen, bedrijfsinformatie, alle niet-publieke informatie over het bedrijf of met gegevens die beschouwd kunnen worden als persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming (bv. persoonsgegevens van klanten, leveranciers en derden). Deze Policy is van toepassing op alle medewerkers van de Vennootschap, inclusief op bestuurders, leden van het management, zelfstandige medewerkers, uitzendkrachten, jobstudenten en stagiaires (hierna: de “Medewerker”).

Met deze Policy wenst de werkgever zijn Medewerkers te informeren over hoe om te gaan met persoonsgegevens en vertrouwelijke informatie om het risico op inbreuken zo klein mogelijk te houden. De Medewerker dient onderstaande richtlijnen nauwgezet na te leven.

2. TOEGANG

De Medewerker krijgt tijdens de uitoefening van zijn functie toegang tot vertrouwelijke Informatie en persoonsgegevens. Deze vertrouwelijke informatie en persoonsgegevens mogen enkel worden gebruikt voor zover noodzakelijk voor de uitoefening van de functie. De Medewerker ziet er strikt op toe dat de vertrouwelijke informatie en persoonsgegevens niet gedeeld worden met onbevoegde personen (incl. onbevoegde collega’s).

De Medewerker verbindt zich er ook toe geen kennis te nemen van vertrouwelijke informatie en persoonsgegevens waarvan hij weet of behoort te weten dat hij geen recht op toegang heeft tot deze informatie.

De Medewerker wendt de vertrouwelijke informatie en persoonsgegevens nooit aan ten nadele van betrokken Vennootschap.

3. VERPLICHTINGEN EN VERANTWOORDELIJKHEDEN

De Medewerker gaat steeds op een voorzichtige en diligente wijze om met vertrouwelijke informatie en persoonsgegevens. Daarbij gelden in het bijzonder de volgende verplichtingen en verantwoordelijkheden:

- Professionele documenten of bestanden mogen alleen bewaard worden op de daartoe voorziene systemen.
- Professionele documenten of bestanden worden niet doorgestuurd naar een private mailbox of naar een derde, tenzij noodzakelijk voor de uitvoering van de activiteiten van de betrokken Vennootschap.
- Elke medewerker is verantwoordelijk voor een correct en voorzichtig paswoordbeheer: paswoorden moeten voldoende gecompliceerd en niet voor de hand liggend zijn en moeten regelmatig (minstens elke zes maanden) gewijzigd worden.
- De pc/laptop wordt automatisch vergrendeld met een wachtwoord wanneer de Medewerker verwacht minstens twee uur afwezig te zullen zijn. Op het einde van de werkdag wordt de pc volledig afgesloten.
- Er wordt zoveel mogelijk gestreefd naar een clean desk policy. Dossiers met vertrouwelijke informatie of persoonsgegevens worden in geval van afwezigheid van langer dan 15 minuten van het bureau verwijderd en op het einde van de werkdag n een vergrendelde kast opgeborgen.
- Laptops, tablets, smartphones, usb-sticks of andere hardware worden bij niet-gebruik gedurende tenminste 15 minuten automatisch vergrendeld en in elk geval op het einde van de werkdag in een vergrendelde kast opgeborgen.
- Printopdrachten worden vertrouwelijk behandeld, wat o.m. betekent dat de Medewerker documenten pas kan afdrukken als hij aanwezig is bij het apparaat en mits gebruik van zijn toegangsbadge, zodat de geprinte documenten niet op de printer blijven liggen.
- Vertrouwelijke informatie en persoonsgegevens worden nooit zomaar bij het oud papier gegooid, maar steeds in de daartoe voorziene papierverbrijzelaar vernietigd.
- Vertrouwelijke informatie en persoonsgegevens worden zo weinig mogelijk buiten de Vennootschap getransporteerd. Transport van documenten moet strikt beperkt zijn tot hetgeen noodzakelijk is voor de uitoefening van de functie, zoals vergaderingen.
- De Medewerkers nemen alle nodige maatregelen opdat vertrouwelijke informatie en persoonsgegevens niet gestolen worden of verloren raken. Zo worden alle mogelijke dragers zoals laptop, tablet, smartphone, usb-stick, etc. niet onbeheerd of onveilig achtergelaten buiten de werkvloer (bv. in de auto). Indien een Medewerker toch geconfronteerd wordt met een verlies of diefstal van dergelijke dragers, dan zal hij zijn leidinggevende of de Verantwoordelijke voor gegevensbescherming binnen de zes uur na het ontdekken verwittigen.
- Wanneer gebruik gemaakt wordt van een wifi-verbinding, zal de Medewerker zich er vooraf van vergewissen dat het een veilig netwerk betreft. Er kan en mag nooit gebruik worden gemaakt van onbeveiligde netwerkverbindingen.

Beveiligingsproblemen of datalekken, evenals het verlies of de diefstal van laptop, tablet, usb-stick, smartphone, etc., moeten onmiddellijk en uiterlijk binnen de zes uur na het ontdekken ervan gemeld worden overeenkomstig de in deze Policy omschreven procedure bij datalekken.

4. PROCEDURE BIJ INBREUKEN OF PERSOONSGEGEVENS / DATALEKKEN

Deze procedure is van toepassing op de Medewerker die een inbreuk op een persoonsgegeven vaststelt of vermoedt.

Een inbreuk op een persoonsgegeven of een datalek is in de zin van de Algemene Verordening Gegevensbescherming (AVG) “een inbreuk op de beveiliging 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 begrip moet ruim worden opgevat en omvat bijvoorbeeld de volgende datalekken:

- hacking / phishing / ransomware;
- offline datalek (papierbak, printer, …)
- e-mail verzonden naar foutief e-mailadres;
- diefstal of verlies usb-stick;
- diefstal of verlies van papieren dossier;
- diefstal of verlies van gsm, laptop, tablet;
- vermindering of wegvallen toegankelijkheid (vb. uitvallen van de server).

De notie persoonsgegeven wordt ingevuld conform de Algemene Verordening Gegevensbescherming (bv. persoonsgegevens van klanten, leveranciers, werknemers, derden). Bij twijfel of iets een persoonsgegeven is, wendt de Medewerker zich onmiddellijk tot de verantwoordelijke voor de gegevensbescherming binnen [naam v/d vennootschap], [naam contactpersoon + contactgegevens].

Bij een datalek moet de volgende procedure worden nageleefd:

FASE 1 – INTERNE MELDING

De Medewerker die een (mogelijk) datalek constateert, meldt dit onmiddellijk en uiterlijk binnen de zes uur na het ontdekken ervan aan de persoon of personen die binnen de betrokken Vennootschap] is/zijn aangeduid als de Verantwoordelijke voor gegevensbescherming (hierna de “Verantwoordelijke voor gegevensverwerking”.

Deze melding gebeurt indien mogelijk via e-mail. De Medewerker vermeldt in zijn e-mail minstens: 1) de aard van het datalek (bv. verlies, geen toegang meer, inbreuk op vertrouwelijkheid); 2) over welke persoonsgegevens het gaat; 3) de mogelijke oorzaak (bv. hacking, verlies, diefstal).

FASE 2 – BEOORDELING, OVERLEG EN REGISTRATIE IN INTERN REGISTER

De persoon aangeduid als Verantwoordelijke voor gegevensverwerking bekijkt de melding na ontvangst meteen en maakt een beoordeling in functie van de aard van het lek en de betrokken persoonsgegevens, de oorzaak en de gevolgen van het datalek. Deze procedure geldt tevens indien een verwerker de betrokken Vennootschap op de hoogte brengt van een datalek.

- *Eerste hypothese: geen datalek / geen persoonsgegevens / geen risico's*

  Indien de melding geen datalek betreft, indien er geen persoonsgegevens zijn gelekt of indien het datalek geen risico inhoudt voor de rechten en vrijheden van de betrokkene(n), zal de Verantwoordelijke voor gegevensverwerking de interne melding rapporteren aan een lid van het management van de betrokken Vennootschap, het lek registreren in het intern "Datalekregister" en de interne melder hiervan op de hoogte stellen. In dat geval neemt de procedure hier een einde.

- *Tweede hypothese: risico's voor betrokkenen of voor de betrokken Vennootschap].*

  Indien het datalek persoonsgegevens bevat en een risico inhoudt voor de rechten en vrijheden van de betrokkenen, of wanneer het datalek aanzienlijke risico's of gevolgen met zich meebrengt voor de betrokken Vennootschap (vb: impact op de IT-infrastructuur, kwaadwillig opzet, gevoelige gegevens of zeer veel gegevens zijn gelekt), zal de Verantwoordelijke voor gegevensbescherming onmiddellijk contact opnemen met een lid van het management om het datalek te bespreken en te evalueren (vb. gevolgen voor de betrokkenen en de betrokken Vennootschap, maatregelen om de gevolgen te beperken en in de toekomst te voorkomen). Indien nodig, roept de Verantwoordelijke voor gegevensbescherming een crisisteam samen, bestaande uit een lid van het management en desgevallend andere personen die nuttig kunnen zijn voor het overleg (vb: IT-verantwoordelijke, CISO, externen, etc.). Van dit overleg wordt een verslag opgemaakt en het datalek wordt tevens geregistreerd in het intern register van de betrokken Vennootschap. Indien er geen risico's worden vastgesteld voor de rechten en vrijheden van de betrokkenen, eindigt de procedure hier. In het tegenovergesteld geval, wordt overgegaan naar fase 3.

FASE 3 – MELDEN AAN DE GEGEVENSBESCHERMINGSAUTORITEIT (GBA)

Indien een risico wordt vastgesteld voor rechten en vrijheden van de betrokkenen, wordt het datalek door de Verantwoordelijke voor gegevensbescherming en na overleg met een lid van het management gemeld aan de GegevensBeschermingsAutoriteit. Dit gebeurt via het formulier zoals voorzien op de website van de GegevensBeschermingsAutoriteit .

De melding gebeurt onverwijld en niet later dan 72 uur na kennisname. Indien de melding later gebeurt of slechts gedeeltelijk, wordt dit gemotiveerd.

De melding bevat de verplichte gegevens zoals voorzien in artikel 33 Algemene Verordening Gegevensbescherming: de aard van het datalek, de categorieën en aantal betrokkenen; de categorieën en het aantal van persoonsgegevens (indien mogelijk); de eventuele gevolgen van het datalek, de maatregelen die het datalek moeten verhelpen en de gevolgen van het datalek moeten vermijden of verminderen.

Indien het datalek geen hoge risico's inhoudt voor de rechten en vrijheden van betrokkenen, neemt de procedure hier een einde. In het tegenovergesteld geval, wordt overgegaan naar fase 4.

FASE 4 – MEDEDELING AAN DE BETROKKENEN

Bij een hoog risico voor de rechten en vrijheden van de betrokkenen, wordt het datalek in principe onverwijld meegedeeld aan die betrokkenen zelf. Deze mededeling bevat overeenkomstig artikel 34 Algemene Verordening Gegevensbescherming een omschrijving, in duidelijke en eenvoudige taal, van de aard van het datalek, de waarschijnlijke gevolgen ervan en de maatregelen die het datalek moeten verhelpen en de gevolgen ervan moeten vermijden of verminderen.

Deze melding hoeft echter niet te gebeuren indien technische en organisatorische maatregelen werden genomen waardoor de gegevens onleesbaar zijn (bv. encryptie, versleuteling) of wanneer maatregelen werden genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van de betrokkenen zich niet meer zal voordoen.

Bij elk datalek wordt het nodige gedaan voor het uitvoeren van de noodzakelijke maatregelen evenals de eventuele noodzakelijke technische en organisatorische maatregelen (vb. aandachtspunten voor de toekomst, oorzaken beperken, defecten en systemen herstellen, infecties verwijderen, …). De Verantwoordelijke voor gegevensbescherming ziet toe op de correcte uitvoering en waakt over de verdere opvolging. Dit alles wordt geëvalueerd en tevens gedocumenteerd.

In geval een datalek gemeld dient te worden aan de GegevensBeschermingsAutoriteit, maakt de Verantwoordelijke voor gegevensverwerking een rapport op dat een weergave biedt van de aard van het datalek, de wijze waarop gehandeld werd, de genomen maatregelen, de betrokken personen en de aandachtspunten naar de toekomst. De Verantwoordelijke voor gegevensverwerking bezorgt dit rapport, na goedkeuring ervan door een lid van het management, aan de leidinggevende persoon/ het leidinggevend orgaan van de betrokken Vennootschap.