Het dagelijks bestuur van Ferm Werk,

Gelet op artikel 34a van de Wet bescherming persoonsgegevens,

Besluit vast te stellen de hierna volgende

Regeling meldplicht datalekken 2016

Artikel 1 Begripsomschrijvingen

In deze regeling wordt verstaan onder:

1. *Werkgever:*
   Ferm Werk GR, Ferm Werk NV, Stichting de Wissel en Stichting Facilitaire Dienstverlening hierna te noemen ieder voor zich of tezamen "werkgever", tenzij uitdrukkelijk anders is bepaald.
2. *Werknemer:*
   Medewerkers met ambtelijke aanstelling of een arbeidsovereenkomst naar burgerlijk recht of bij een van de in lid 1 van dit artikel genoemde werkgevers. Stagiaires worden in deze regeling ook als werknemer aangemerkt.
3. *Betrokkene:*
   Betrokkene is degene van wie persoonsgegevens zijn gelekt.

Artikel 2 Doel en reikwijdte

De regeling meldplicht datalekken heeft als doel:

- Duidelijkheid geven wat datalekken zijn en hoe daar mee om te gaan.
- Werknemers op de hoogte te brengen van de meldplicht.
- Maatregelen en voorzieningen treffen om datalekken te voorkomen o.a. door gegevens goed te beveiligen.
- Voorkomen van sancties voor de werkgever op niet-naleving van de meldplicht.
- Bij incidenten adequate maatregelen te treffen om verdere datalekken te voorkomen.

De verplichtingen zijn van toepassing op de werkgever niet op de bewerker. Het is aan de werkgever om te beoordelen of een datalek voldoet aan de meldplicht.

Artikel 3 Datalekken

3.1. Wat is een datalek?

We spreken van een datalek als persoonsgegevens in handen vallen van derden, die geen toegang tot die gegevens zouden mogen hebben. Een datalek kan het gevolg zijn van een beveiligingsprobleem. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een gestolen of verloren geprinte klantenlijst evengoed een datalek vormen. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens, zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens. Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking - dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

3.2. Voorbeelden datalekken

Bij beveiligingsincidenten waar sprake kan zijn van een inbreuk op de beveiliging van persoonsgegevens moet u bijvoorbeeld denken aan:

- een kwijtgeraakte USB-stick;
- een gestolen laptop;
- een inbraak door een hacker;
- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum.

Kenmerkend voor een inbreuk op de beveiliging is verder dat het beveiligingsincident daadwerkelijk gevolgen heeft voor de persoonsgegevens die worden verwerkt. Er zijn persoonsgegevens verloren gegaan, of redelijkerwijs kan niet worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt. De beveiligingsmaatregelen en de herstelmaatregelen die getroffen zijn, waren niet voldoende om deze gevolgen geheel weg te nemen.
Naast het verliezen van een ICT-middel of een beveiligingsincident in een ICT-systeem zijn er ook analoge incidenten die onder deze wetgeving vallen. Denk aan een brief of formulier met daarop persoonsgegevens die kwijt raakt of gestolen is. Het onjuist verwerken van persoonsgegevens of het kwijt raken van persoonsgegevens, maar er is geen back-up voor handen, wordt als een datalek gezien. Je moet immers opnieuw aan betreffende persoon zijn gegevens opvragen.

3.2.1. Voorbeeld van analoge datalek
Een envelop met creditcardbetalingsgegevens van 800 personen was per ongeluk niet versnipperd, maar in een vuilnisbak gegooid. Een derde persoon haalde de gegevens uit de vuilniscontainer op straat en verstrekte ze aan andere personen. Het datalek kan financiële consequenties hebben voor de betrokkenen, als hun kaartgegevens nog geldig zijn en worden misbruikt. De betrokkenen moeten daarom van het datalek in kennis worden gesteld.

3.2.2. Voorbeeld technische beschermingsmaatregelen bij verlies van persoonsgegevens
De versleutelde laptop van een financieel adviseur is gestolen uit de kofferbak van zijn auto. Op de laptop staan de financiële dossiers - met daarin onder meer details over hypotheken, salarissen en aanvragen van leningen - van 1000 betrokkenen.
Door de diefstal zijn deze gegevens blootgesteld aan onbevoegde kennisname. De financieel adviseur komt tot de conclusie dat alle gegevens op de harde schijf adequaat versleuteld zijn, en dat het restrisico acceptabel is. In principe zou hij de melding aan de betrokkene dus achterwege kunnen laten.
Echter: De financieel adviseur beschikt niet over een back-up (reserve-kopie) van de persoonsgegevens op de harde schijf. Dat betekent dat er in dit geval niet alleen sprake is van blootstelling aan onbevoegde kennisname, maar ook van het verlies van de getroffen persoonsgegevens.
Aangezien de financieel adviseur de gegevens niet meer heeft, zal hij ze opnieuw bij de betrokkenen op moeten vragen. De vertraging die hierdoor ontstaat kan ertoe leiden dat deadlines voor de indiening van documenten of aanvragen niet worden gehaald, wat voor de betrokkenen uiteindelijk kan leiden tot boetes, derving van inkomsten of verwachte winst, beëindiging van koopovereenkomsten of andere ingrijpende gevolgen.

In dit geval ligt het, ondanks de genomen technische beschermingsmaatregelen, voor de hand om het datalek te melden aan de betrokkenen. De melding omvat in ieder geval het verzoek om de gegevens opnieuw aan de financieel adviseur te verstrekken en een uitleg van de potentiële consequenties en negatieve gevolgen van de inbreuk.

Artikel 4 Persoonsgegevens

4.1. Wat zijn persoonsgegevens
Persoonsgegevens geven directe of indirecte informatie over een persoon. Deze persoon moet daarbij wel te identificeren zijn. Dit is geregeld in de Wet bescherming persoonsgegevens (Wbp). Deze wet geeft regels ter bescherming van persoonsgegevens.

4.2. Directe persoonsgegevens
Sommige persoonsgegevens geven directe en feitelijke informatie over een persoon. Bijvoorbeeld iemands Burger Service Nummer (BSN), geboortedatum, emailadres, adres of geslacht. Dit geldt ook voor gegevens die een waardering geven over een bepaalde persoon. Een voorbeeld hiervan is iemands IQ.

4.3. Indirecte persoonsgegevens
Er zijn ook gegevens die indirect iets vertellen over een bepaald persoon. Bijvoorbeeld over de maatschappelijke status van deze persoon. Zo zegt de winst van een eenmanszaak iets over het

inkomen van haar eigenaar. Als deze gegevens zijn te herleiden tot een bepaalde persoon is sprake van persoonsgegevens.

4.4. Bijzondere gegevens

Bijzondere persoonsgegevens zijn onder andere gegevens over iemands:

- Ras;
- godsdienst of levensovertuiging;
- politieke gezindheid;
- gezondheid;
- strafrechtelijke verleden;
- seksuele leven;
- lidmaatschap van een vakvereniging.

Ook strafrechtelijke persoonsgegevens zijn bijzondere gegevens. Het gaat dan bijvoorbeeld om informatie over misdrijven, overtredingen en veroordelingen.

Artikel 5 Verwerken persoonsgegevens

5.1. Wat houdt verwerken van persoonsgegevens In

Verwerking van persoonsgegevens betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1, sub b, Wbp).

5.2. Onrechtmatig verwerken van persoonsgegevens

Onder onrechtmatige vormen van verwerking vallen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan. Als u redelijkerwijs niet kunt uitsluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet u de inbreuk beschouwen als een datalek.
Bij een malware-besmetting moet u ervan uitgaan dat er sprake kan zijn van een datalek. Bepaalde typen malware doorzoeken de besmette apparatuur op waardevolle persoonsgegevens om de gevonden gegevens vervolgens weg te sluizen naar een server die in handen is van de aanvaller. Denk hierbij aan e-mailadressen, gebruikersnamen en wachtwoorden en creditcardgegevens. Een dergelijke malware-besmetting stelt de getroffen persoonsgegevens dus bloot aan onbevoegde kennisname en andere vormen van onrechtmatige verwerking.

5.3. Voorbeeld wel / geen datalek (onrechtmatige verwerking van persoonsgegevens)

Een werknemer geeft aan een derde de gebruikersnaam en het wachtwoord die toegang geven tot alle klantgegevens van alle klanten van het bedrijf waar hij werkt.
Na ontdekking van het gebeurde past het bedrijf het wachtwoord van het betreffende account aan, zodat de derde geen toegang meer heeft.
Daarna onderzoekt het bedrijf of de derde daadwerkelijk toegang heeft gezocht tot de klantgegevens. Bij dit onderzoek maakt het bedrijf gebruik van logbestanden, waarin per gebruikersnaam is vastgelegd welke acties er op welk tijdstip zijn uitgevoerd met welke klantgegevens.
Als op basis van de logbestanden redelijkerwijs kan worden uitgesloten dat er door middel van het betreffende account toegang is verkregen tot de klantgegevens, dan is er uitsluitend sprake van een beveiligingslek en niet van een datalek.

Artikel 6 Meldplicht datalek (prodedure)

De werknemer is verplicht een datalek binnen 24 uur na ontdekking te melden aan de verantwoordelijke manager binnen Ferm Werk (zie toelichting).

6.1 Taken, verantwoordelijkheden en bevoegdheden

1. Iedere medewerker die direct of indirect kennis draagt of krijgt van een privacy lek, is verplicht dit direct te melden aan zijn eigen manager en de manager Financiën en ICT.
2. De manager Financiën en ICT is verantwoordelijk voor het onderzoeken van het incident;
3. Het Afdelingsmanager is verantwoordelijk voor het ondernemen van preventieve en repressieve acties;
4. De manager Financiën en ICT is verantwoordelijk voor de actualiteit van deze procedure.

6.2 Uitvoering

1. De medewerker die direct of indirect kennis draagt of krijgt van een incident inzake het lekken van privacygegevens meldt dit direct zijn eigen manager en de manager Financiën en ICT.
2. De manager Financiën en ICT, eventueel in samenwerking met de afdelingsmanager onderzoeken het incident. Hierbij is aandacht voor de volgende aspecten:
    a. wat is de aard van het privacylek;
    b. wat is de oorzaak dat dit incident heeft plaatsgevonden;
    c. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
    d. is de organisatie verwijtbaar;
    e. van het incident wordt een verslag gemaakt en in Alfresco vastgelegd;
3. De manager Financiën en ICT neemt contact op met de Autoriteit Persoonsgegevens en aan de hand van het verslag wordt uitleg gegeven;
4. Eventuele aanwijzingen van de Autoriteit Persoonsgegevens worden vastgelegd en opgevolgd.

6.3 Interne controle

1. Op basis van de, gedurende een jaar, ontvangen meldingen analyseert de manager Financiën en ICT deze en stelt een verbeterplan of -advies op. Dit plan of advies wordt opgenomen in de jaarlijks uit te brengen managementrapportage;
2. Minimaal jaarlijks beoordeelt de manager Financiën en ICT of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de procedure.

6.4 Melden aan Autoriteit Persoonsgegevens (AP)

Niet ieder datalek moet gemeld worden aan de Autoriteit Persoonsgegevens. Volgens de wet moet een melding gedaan worden aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Ferm Werk hoeft een datalek alleen te melden als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Of als een aanzienlijke kans bestaat dat dit gebeurt.

Artikel 7 Logboek met datalekken bijhouden

Ferm Werk heeft de plicht een logboek bij te houden van alle lekken die ernstig genoeg waren om aan de Autoriteit Persoonsgegevens te moeten melden. Preciezer geformuleerd (art. 34a):
"De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene."

Artikel 8 Inwerkingtreding

Deze regeling treedt in werking met ingang van 1 september 2016.

Artikel 9 Citeertitel

Deze regeling kan worden aangehaald als "Regeling meldplicht datalekken 2016".

Aldus vastgesteld door het dagelijks bestuur van Ferm Werk in zijn vergadering van 15 december 2016.

Y. Koster-Dreese
Voorzitter dagelijks bestuur Ferm Werk
B.F. Drost
Secretaris dagelijks bestuur Ferm Werk

Toelichting op artikelen

Vanaf 1 januari 2016 heeft het College Bescherming Persoonsgegevens (CBP) een nieuwe naam: Autoriteit Persoonsgegevens (AP).

Artikel 6 Melden van een datalek binnen FERM WERK

Het melden van een datalek dient direct na ontdekking plaats te vinden bij de manager Financiën & ICT. Deze manager zal samen met de melder aan de hand van de opgestelde checklist van de Autoriteit Persoonsgegevens nagaan of de melding voldoet aan de meldplicht. Indien dit het geval is zal de melding worden besproken met de directeur voor verdere afhandeling van het incident.

Artikel 6.1 Melden aan de betrokkene

Als Ferm Werk tot de conclusie komt dat een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens, dan betekent dit niet automatisch dat dit datalek ook gemeld moet worden aan de betrokkene. Ferm Werk moet hiervoor een aparte afweging maken.

Artikel 6.2 Melden aan de Autoriteit Persoonsgegevens

Ferm Werk moet de melding van een datalek doen zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar.