PROTOCOL DATALEKKEN COOL KUNST EN CULTUUR

Cool kunst en cultuur heeft een Data Protection Officer. Dat is Paul Schermer.
De DPO is bereikbaar via paul@coolkunstencultuur.nl

1. Definities datalekken

De volgende definities zijn gebaseerd op de richtsnoeren meldplicht datalekken van de autoriteit persoonsgegevens. De Data Protection Officer moet deze definities kennen en toepassen.

Een **incident** is een concrete gebeurtenis waarbij de beschikbaarheid, confidentialiteit of integriteit van een informatie-asset is geschonden. Niet elk incident is een datalek.

Een **datalek** is een incident waarbij er persoonsgegevens verloren zijn gegaan of als er onrechtmatige verwerking heeft plaatsgevonden.

Een **persoonsgegeven** is elk gegeven dat herleidbaar is tot een natuurlijk persoon. Denk aan email, telefoonnummer, voornaam_achternaam, huisadres, kenteken, IP-nummer, bankrekeningnummer, MAC-adres, foto's met gezichten erop, inkomen, geboortedatum. Niet persoonsgegevens zijn gemiddeldes over grotere groepen.

2. Melden van datalekken aan DPO

Elk beveiligingsincident moet worden gemeld bij de Data Protection Officer. Hij bepaalt of er sprake is van een datalek. Bij twijfel wordt er door de DPO overlegd met MT of directie

Iedereen in de organisatie die werkt met persoonsgegevens, moet weten dat er een meldplicht datalekken is en dat zij een incident of datalek direct moeten melden. Daartoe wordt dit opgenomen in het personeelshandboek en opgehangen in de personeelsruimte.

3. Acties DPO

Vastleggen en uitzoeken: De DPO logt het incident, bestudeert het incident. Zoek uit wat er wanneer en waar is gebeurd en welke apparatuur en partijen hierbij betrokken zijn geweest. Indien de DPO niet aanwezig is, dan gebeurt dit door een andere vertegenwoordiger van de afdeling Techniek in overleg met de afdeling Communicatie.

Directe actie: Indien nodig, neem direct actie om het lek te dichten of te stoppen. Denk aan uitzetten servers, blokkeren accounts of verwijderen gevoelige data. Indien nodig worden externe verwerkers ingeschakeld zoals *Cursad* of *Get-a-Ticket* danwel bij Cool betrokken externe ICT-dienstverleners zoals *Herke* of *Basic Orange.*

Besluit persoonsgegevens: De DPO bepaalt samen met de betrokken afdelingen welke persoonsgegevens van hoeveel en welke personen er betrokken zijn. Als uitkomst hiervan wordt het aantal personen vastgelegd, welke soorten gegevens en of er sprake is van bijzondere gegevens.

Bepaal de verantwoordelijke: De DPO bepaalt samen met de betrokken afdelingen wie de verantwoordelijke voor de gegevens is. Dit wordt bepaald door na te gaan hoe de gegevens zijn verkregen en door bestudering van alle bewerkers-overeenkomsten waaronder de gegevens zijn doorgegeven. De verantwoordelijk kan een klant zijn, of Cool als organisatie zelf.

Bepaal uitsluitbaarheid: Soms is het redelijkerwijs uit te sluiten is dat persoonsgegevens onrechtmatig zijn verwerkt. Dit is bijvoorbeeld het geval bij diefstal van een laptop die voorzien is van

sterke encryptie. Goede encryptie leidt tot uitsluitbaarheid. Zonder goede encryptie is er geen uitsluitbaarheid.

4. Melding als een externe verwerker verantwoordelijk is

Als de organisatie Cool zelf niet de verantwoordelijke is, wordt er door de DPO melding gedaan conform de contactgegevens in bewerkersovereenkomst. Indien dit niet duidelijk is of niet uitvoerbaar, wordt contact opgenomen via telefoonnummer op website van partij. Het streven is om dit te doen binnen 8 kantooruren na ontdekking incident (of conform termijn in bewerkersovereenkomst). De verantwoordelijke moet zorgen voor de overige meldingen. De organisatie volgt verder alleen de instructies van de verantwoordelijke.

In overleg met directie en de afdeling Communicatie wordt bepaald of bezoekers, deelnemers of werknemers van Cool dienen te worden geïnformeerd. Zo ja, dan treedt artikel 6 in werking.

5. Melding als Cool zelf de verantwoordelijke is

Als er sprake is van een niet uitsluitbaar datalek en de organisatie verantwoordelijke is, dan onderneemt de DPO de volgende stappen:

- Op de hoogte brengen van directie, MT en de afdeling Communicatie
- Afronden onderzoek en goed vastleggen uitkomsten in een apart incidentrapport
- Inschatten ernst incident: Een incident is ernstig als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Een incident met gevoelige persoonsgegevens is altijd ernstig, ook met 1 persoon. Een incident zonder gevoelige persoonsgegevens is ernstig bij een voldoende omvang.
- Als het datalek ernstig is, dan moet het incident via het webformulier gemeld worden bij de Autoriteit Persoonsgegevens. Dit moet indien mogelijk binnen 72 uur na ontdekking.
  De afbeelding hieronder, afkomstig uit de richtsnoeren, laat de voorbeelden zien van datalekken die moeten worden gemeld.

Voorbeelden van datalekken die moeten worden gemeld aan de Autoriteit Persoonsgegevens (1)[17]

- Intern wordt binnen een ziekenhuis gesignaleerd dat door een haperende beveiliging (technische storing) medische gegevens zijn ingezien door onbevoegden;
- Een journalistiek programma confronteert een bedrijf met het feit dat als gevolg van een beveiligingslek onder andere persoonlijke gegevens (zoals kopieën van paspoorten of rijbewijzen, bankgegevens en wachtwoorden) van werknemers op de server van het bedrijf door onbevoegden zijn ingezien;
- Een medewerker verliest een laptop met onversleutelde, financiële klantgegevens;
- Een bedrijf krijgt te maken met een hack waarbij klantgegevens en wachtwoorden zijn ontvreemd;
- Een overheidsdatabase met gevoelige persoonsgegevens wordt gehackt waardoor onbevoegden toegang hebben gekregen tot deze gegevens.

De melding wordt samen met de directeur-bestuurder gedaan.

6. Communicatie

De afdeling Communicatie verzorgt bij een ernstig datalek de volgende stappen:

- Via een bericht op de website en via de eigen social media wordt melding gemaakt van het datalek. Er wordt gemeld om welke gegevens het gaat, of het lek inmiddels is gedicht, welke stappen er ondernomen en nog te nemen zijn.
- De betrokken personen (zoals deelnemers, toeschouwers of werknemers) worden via een persoonlijke mail op de hoogte gesteld over het datalek. Ook hier wordt gemeld om welke

gegevens het gaat, of het lek inmiddels is gedicht, welke stappen er ondernomen en nog te nemen zijn.
- Indien de aard van het datalek dusdanig is dat het imago van de organisatie kan worden geschaad, dan houdt Cool het initiatief in de Communicatie. De afdeling zal in dat geval in nauw overleg met directie en MT via een officieel bericht de lokale media en stakeholders informeren.

7. Evaluatie

De DPO denkt na over verbeteringen die toekomstige datalekken kunnen voorkomen. Dit gebeurt in overleg met betrokken externe verwerkers zoals *Cursad* of *Get-a-Ticket* danwel met bij Cool betrokken externe ICT-dienstverleners zoals *Herke* of *Basic Orange.*

Dit protocol is opgesteld op 21 maart 2018 en zal jaarlijks worden geëvalueerd en indien nodig aangepast.