Formulier : Melden datalek

Voor het melden van (het vermoeden van) een datalek vult u onderstaand formulier in. Na invulling kunt u dit formulier als PDF opslaan en als bijlage digitaal zenden naar: info@activus.nl

Of sturen per gewone post naar:

Activus Technisch Personeel BV / Actief Diensten en Detachering BV
Ridderplein 31
5421 CX Gemert

- Naam en contactgegevens van de melder en waar meer informatie kan worden verkregen:
- Samenvatting van het Beveiligingsincident dat de inbreuk in verband met persoonsgegevens heeft veroorzaakt (met inbegrip van de fysieke locatie waar de inbreuk plaatsvond en de betrokken opslagmedia).
- De aard van de inbreuk op de persoonsgegevens.
- Datum en tijdstip van het incident (eventueel bij benadering) en van het moment waarop dit werd vastgesteld:
    - Datum:
    - Tussen (begindatum periode) en (einddatum periode)
    - Nog niet bekend
- Omstandigheden van de inbreuk in verband met persoonsgegevens (bv. diefstal, verlies kopiëren):
    - Lezen (vertrouwelijkheid)
    - Kopiëren
    - Veranderen (integriteit)
    - Verwijderen of vernietigen (beschikbaarheid)
    - Diefstal
    - Nog niet bekend
- Type persoonsgegevens:
    - Naam
    - Geslacht
    - Geboortedatum en/of leeftijd
    - Bijzondere persoonsgegevens (bijv. ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
    - Adres
    - Telefoonnummer(s)
    - E-mailadres(sen) of ander(e) adres(sen) voor elektronisch communicatie
    - Toegangs- of identificatiegegevens (bijv. inlognaam, wachtwoord en klantnummer)
    - Financiële gegevens (bijv. IBAN en creditcardnummer)
    - Burgerservicenummer of sofinummer
    - Legitimatiebewijskopieën (bijv. kopie paspoort)
    - Overige gegevens, namelijk:
- Hoeveelheid Betrokkene betrokken bij het Beveiligingsincident:
    - Minimaal:
    - Maximaal:

- Omschrijving Betrokkene van wie persoonsgegevens zijn betrokken bij het Beveiligingsincident:
- De categorie en mogelijk aantal records van persoonsgegevens:
- Potentiële gevolgen van het Beveiligingsincident:
    - Stigmatisering of uitsluiting
    - Schade aan de gezondheid
    - Blootstelling aan (identiteits)fraude
    - Blootstelling aan spam of phishing
    - Anders, namelijk:
- Maatregelen die met betrekking tot de persoonsgegevens door de aanbieder zijn (of worden) toegepast:
- Maatregelen die reeds zijn genomen of voorgesteld worden om te nemen teneinde het Beveiligingsincident op te lossen en te voorkomen in de toekomst:
- Maatregelen die reeds zijn genomen of voorgesteld worden om te nemen teneinde de gevolgen van het Beveiligingsincident zoveel mogelijk te beperken en inzichtelijk te krijgen:
- Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?
    - Ja, namelijk op de volgende wijze:
    - Nee, omdat:
    - Deels, namelijk :

    *Als de persoons gegeven geheel of deel onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)
- Heeft het Beveiligingsincident betrekking op Betrokkene in andere landen dan binnen de EER?
    - Ja, namelijk:
    - Nee, alleen in Nederland/België/Frankrijk/Duitsland/…
    - Nog niet bekend.
- Alle overige door Verwerkingsverantwoordelijke gevraagde informatie:

Ondertekening

Met de ondertekening verklaart u bevoegd te zijn deze melding te doen en dat de in de melding verstrekte informatie juist is.

Datum:

Handtekening: