



Factsheet

Jaaroverzicht datalekken 2020

Introductie

Sinds 2016 geldt in Nederland de meldplicht datalekken. Organisaties moeten een overzicht van datalekken bijhouden en het datalek melden aan de Autoriteit Persoonsgegevens (AP) en aan de getroffen personen wanneer het datalek een hoog risico oplevert voor de persoonsgegevens. Deze rapportage geeft inzicht in het aantal en de soort datalekken die Justis in 2020 heeft afgehandeld.

Aantal meldingen

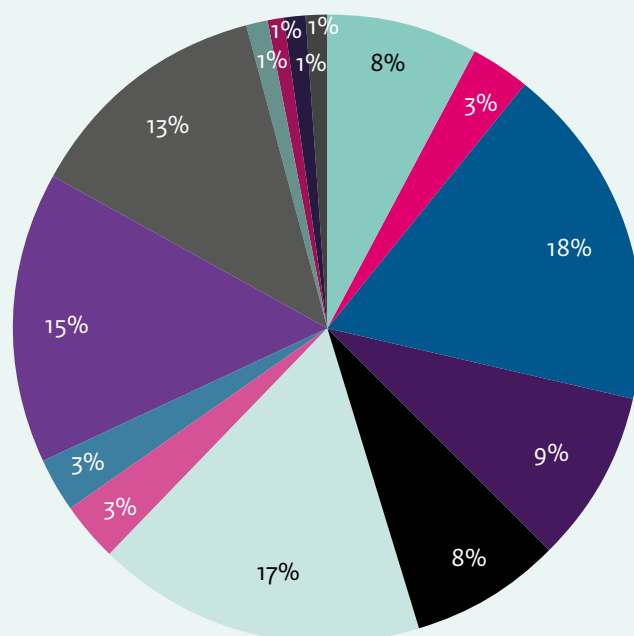
78

Aantal datalekken gemeld bij Autoriteit
Persoonsgegevens en betrokkenen

14

Type datalekken

- Brief naar oud adres (tussentijdse verhuizing niet doorgegeven door aanvrager) (6).
- Meerdere brieven in een enveloppe (2).
- Typefout of verkeerd adres gebruikt (14).
- Persoonsverwisseling (7).
- E-mail of brief met onjuiste gegevens naar betrokkene (6).
- Gegevens naar onjuist e-mailadres (13).
- Informatieverzoek aan informatieleverancier met meer informatie over betrokkene dan strikt noodzakelijk (2).
- Informatieverzoek aan informatieleverancier bevat per abuis ook informatie over andere personen (2).
- Enveloppe geopend retour ontvangen terwijl adres klopt (12).
- Onrechtmatige verstrekking of verwerking (10).
- Brief terecht gekomen bij een derde terwijl adres klopt (1).
- Aanvraag of dossier niet meer gevonden (1).
- Aangetekend poststuk niet ontvangen (1).
- Per abuis geen toestemming gevraagd (1).



Toelichting

In bovenstaande figuur zijn de 78 datalekken uit 2020 verdeeld naar type datalek. Het betreft onder meer datalekken als gevolg van verkregen onjuiste gegevens, door menselijke fouten en datalekken met een onduidelijke oorzaak.

De 14 datalekken die bij de AP en bij betrokkene zijn gemeld, zijn verdeeld over de genoemde typen datalekken. Het gaat met name om gevallen waarin brieven met strafrechtelijke persoonsgegevens mogelijk bij een derde terecht zijn gekomen. Daarnaast komt naar schatting 0,8% van het aantal afgegeven Verklaringen Omtrent het Gedrag niet per post aan bij de aanvrager. Dit kan verschillende oorzaken hebben, zoals een verhuizing, zoek raken bij PostNL, een fout in de adressering, etc.

Corrigerende maatregelen:

- Justis heeft derden gevraagd de e-mail te verwijderen of de brief te retourneren of te vernietigen.
- Justis heeft een brief met juiste gegevens verstuurd, of een brief verstuurd naar het juiste post- of e-mailadres.
- Justis is in gesprek gegaan met betrokkene om toelichting te geven en excuses aan te bieden.
- Justis heeft gecontroleerd wat het risico is van de gelekte gegevens.
- Justis heeft gegevens opgevraagd bij PostNL om meer duidelijkheid te krijgen over de oorzaak van het datalek.

Preventieve maatregelen:

- Justis wijst medewerkers op het belang van zorgvuldigheid en controle.
- Justis bespreekt de casus op de afdeling om herhaling te voorkomen.
- Justis communiceert dat contactpersonen voor een mailing altijd moeten worden vermeld in 'BCC', niet in 'Aan'.
- Justis scherpt de procedure Klanttevredenheidsonderzoek aan om te garanderen dat men van tevoren wordt gebeld om toestemming te vragen voor het benaderen voor Klanttevredenheidsonderzoek.
- Justis geeft voorlichting op afdelingen om bewustwording te verhogen.
- Justis is bezig met een pilot Robotic Automation Proces om adressen geautomatiseerd te laten controleren in de Basisregistratie persoonsgegevens (BRP) alvorens brieven met gevoelige informatie te verzenden.

Colofon

Dit is een publicatie van:
Justis

Februari 2021 | 21401423