gemeente
NOORDOOSTPOLDER

Rapportage Informatieveiligheid, AVG en Wpg 2023

Gemeente Noordoostpolder

Inleiding

- Onze inwoners, ondernemers en samenwerkingpartners moeten erop kunnen vertrouwen dat hun (persoons)gegevens bij ons in vertrouwde handen zijn.

- Daarom stellen we eisen aan de bescherming van onze gegevens èn aan het waarborgen van de privacy van onze inwoners.

- Dat doen we vanuit de wetenschap dat het vooraf goed inrichten van informatiebeveiliging extra tijdsinvestering en herstelkosten achteraf helpt te voorkomen.

Wat willen we bereiken?

gemeente NOORDOOSTPOLDER

Onze inwoners moeten er op kunnen vertrouwen dat hun gegevens bij ons veilig zijn en dat hun privacy gerespecteerd wordt.

- **Gegevens moeten op orde en controleerbaar zijn**
- **Gegevens en informatie mogen alleen verwerkt worden als ze nodig zijn voor uitvoering van onze gemeentelijke taken**
- **Gegevens en informatie mogen alleen beschikbaar zijn voor de daartoe geautoriseerde personen**
- **Gegevens moeten voor hen beschikbaar zijn en mogen niet onderschept, gelezen of gemanipuleerd kunnen worden**
- **Medewerkers moeten zorgvuldig en bewust handelen om bovenstaande te borgen.**
- **Doelstellingen en beginselen uit de AVG moeten we waarborgen**
- **Onze toezichthouders moeten voldoen aan de Wet politiegegevens**

Kaders en richtlijnen

gemeente NOORDOOSTPOLDER

- Voor gemeenten is de Baseline Informatiebeveiliging Overheid (BIO) een belangrijk verplicht kader.
- De Wet digitale overheid regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi)overheid.
- De 10 principes voor informatiebeveiliging van de VNG zijn een bestuurlijke aanvulling hier op.
- Specifiek met betrekking tot bescherming van persoonsgegevens zijn de Algemene verordening gegevensbescherming (AVG) en de Nederlandse uitvoeringswet (uAVG) leidend.
- Voor toezichthoudende taken in handhaving en het sociaal domein is voor strafrechtelijke zaken de Wet politiegegevens (Wpg) van toepassing.

Dreigingsbeeld 2023-2024

Grootste risico's voor gemeenten:

- **Uitval van dienstverlening en bedrijfsvoering**
- **Vertrouwelijke informatie in verkeerde handen**
- **Fouten in dienstverlening**

Actueel dreigingsbeeld

- Meer ransomware, destructievere gevolgen
- Steeds meer en ernstiger kwetsbaarheden in software
- Gevaren in ketens uit het zicht

Continue doorontwikkelen is nodig

gemeente NOORDOOSTPOLDER

Hackers zitten niet stil, beveiligingsmaatregelen moeten telkens aangepast worden om voldoende weerbaar te blijven.

Aandacht voor privacy

gemeente NOORDOOSTPOLDER

Door:

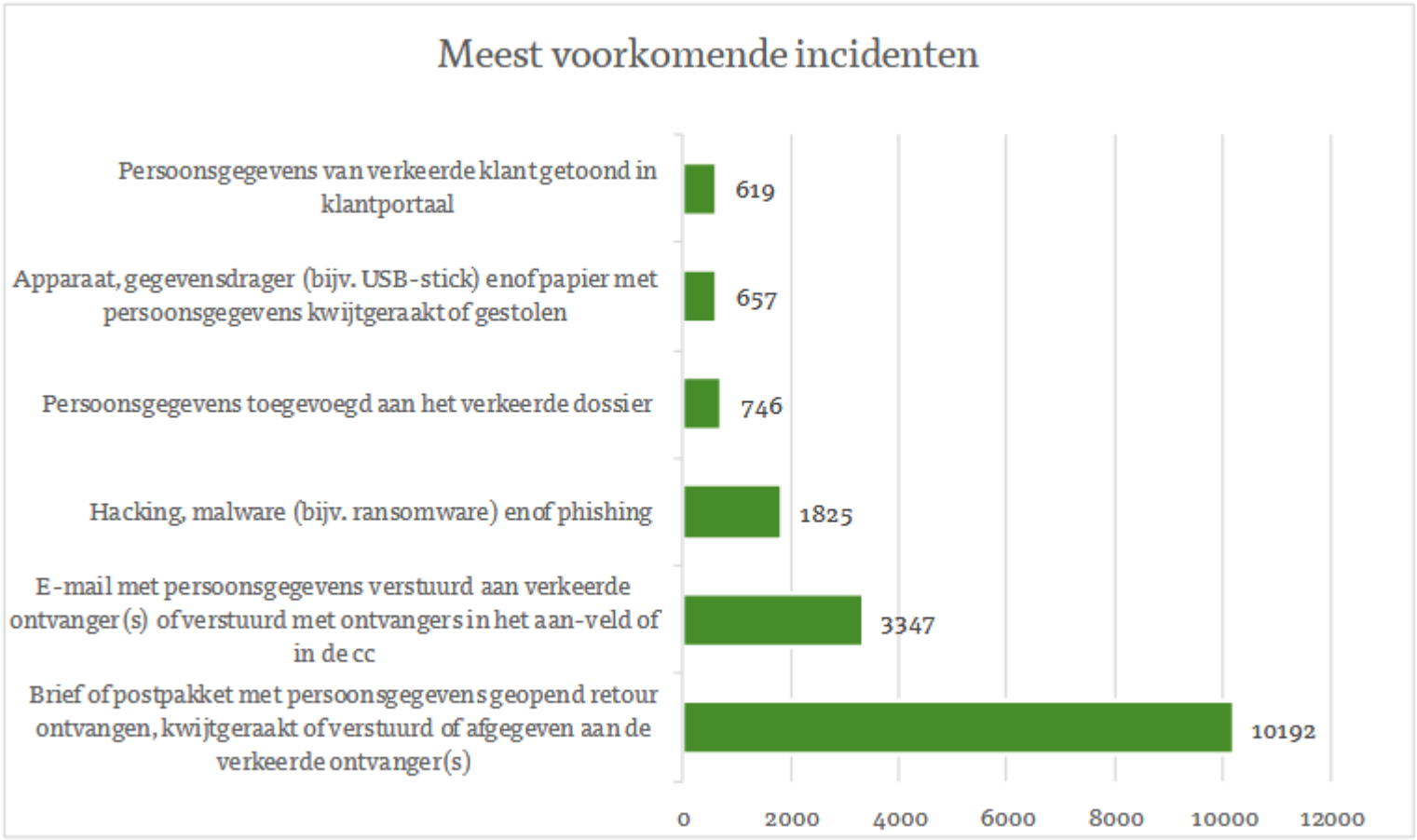
- **Aandacht te vragen om datalekken te melden**
- **Privacy impact analyses uit te voeren**
- **Bij wijzigingen in verwerkingen en systemen informatieveiligheid en privacy vanaf de start mee te nemen (privacy by design en default)**
- **Bij inkooptrajecten direct aandacht te vragen voorbeveiligingseisen en verwerkersovereenkomsten**
- **Aansluiten bij het nationale algoritmeregister**
- **Extra aandacht voor processen die onder de Wpg vallen**

Centrale boodschap Autoriteit Persoonsgegevens

Ga ervan uit dat er al eens persoonlijke gegevens van je gelekt zijn, of dat dit nog gaat gebeuren. Maak daarom werk van het beschermen van je persoonsgegevens.

Datalekkenrapportage AP

gemeente NOORDOOSTPOLDER



Landelijk bijna 15.000 meldingen hier over,

Incidenten en datalekken in Noordoostpolder

gemeente NOORDOOSTPOLDER

Kwetsbaarheid meldingen IBD	Melding incident of datalek	Datalek	Melding AP	Inzage Verzoek
124	24	11	3	2 AVG 0 Wpg

In 2023 ontvingen we:

- 124 kwetsbaarheidsmeldingen van de IBD op basis van onze geactualiseerde ICT-foto. Deze zijn getoetst en waar nodig zijn maatregelen getroffen.
- 24 meldingen van onze medewerkers over beveiligingsincidenten en potentiële datalekken. Een aantal maal betrof dit CEO-phishing. Allen met een verwaarloosbare impact op onze bedrijfsvoering.
- 11 maal was sprake van een datalek, 3 met een meldplicht richting de Autoriteit Persoonsgegevens. Betrokkenen zijn in voorkomende gevallen geïnformeerd.
- Rechten van betrokkenen: Er is 1 inzageverzoek en 1 verwijderingsverzoek ontvangen en gehonoreerd.

Incidenten en datalekken in Noordoostpolder

De datalekken in 2023:

- **E-mail of brief naar verkeerde (e-mail)adres gestuurd**
- **Stukken naar juiste ontvanger maar in bijlage te veel of verkeerde persoonsgegevens opgenomen**
- **Te veel mensen toegang tot gegevens (overzichten personeelssysteem)**

Met als gevolg:
Mogelijk onbevoegde kennisname van persoonsgegevens door derden. In de meeste gevallen betrof het:

- **Een beperkt aantal betrokkenen**
- **Een beperkt aantal persoonsgegevens**

Alleen stempassen die in november 2023 op onjuiste adressen werden bezorgd, was aanzienlijk qua grootte.

Wet politiegegevens

gemeente NOORDOOSTPOLDER

Verplichte externe audit ter verantwoording over ons gebruik van politiegegevens aan de Autoriteit persoonsgegevens. Van toepassing voor onze BOA's en leerplichtambtenaren

- **In 2023 hercontrole uitgevoerd naar de opzet en het bestaan van de beheersingsmaatregelen die in de wettelijk verplichte externe audit over 2022 als 'voldoet deels' of 'voldoet niet' zijn beoordeeld.**
- **Grote verbeterslag is in opzet van procedures en maatregelen doorgevoerd.**
- **Jaarlijks wordt hier intern op geaudit, eens in de 4 jaar vindt externe toetsing plaats.**

Programma iBewust

Aandacht voor door de menselijke factor.

- **Nieuwe medewerkers doen een e-learning over informatieveiligheid binnen 3 maanden.**
- **5 maal is via introductiedagen aandacht gevraagd voor informatieveiligheid en privacybewust handelen bij nieuwe medewerkers**
- **We blijven op intranet periodiek aandacht vragen informatieveiligheid en en het melden van datalekken**
- **We berichten over actualiteiten rondom fraude, phishing, hack en ransomware via de reguliere kanalen.**

Overige noemenswaardige ontwikkelingen

Kwaliteitsmonitor voor de BRP en de Reisdocumenten doorlopen (zelfevaluatie). Controle antwoorden reisdocumenten door ministerie met akkoord.

ENSIA-verantwoording 2022 afgerond met een collegeverklaring als basis voor verantwoording richting Rijksoverheid

ENSIA-verantwoording 2022 doorlopen met externe audits op de DigiD en Suwinet-inkijk en zelfaudits Informatieveiligheid, WOZ, BAG, BRO en BGT.

Strategisch beleid informatieveiligheid en privacy geactualiseerd, als kader hoe we omgaan met persoonsgegevens en veiligheid.