
PRIVACYPROTOCOL TEN BEHOEVE VAN DE SAMENWERKING TUSSEN DE GEMEENTE (.....NAAM GEMEENTE.....) EN (...NAAM CONTRACTPARTNER.....) BIJ DE UITVOERING VAN DE WET INBURGERING.

In dit protocol leggen partijen vast hoe zij in het kader van de onderhavige Overeenkomst zullen omgaan met persoonsgegevens om te voldoen aan de privacywetgeving, zoals vastgesteld in de Algemene Verordening Gegevensbescherming (AVG).

Artikel 1 – Begrippen

De hierna en hiervoor gebruikte begrippen zijn overeenkomstig met artikel 4 van de AVG.

Artikel 2 - Totstandkoming, duur en beëindiging van het Privacyprotocol

1. Dit protocol treedt in werking op de datum waarop Partijen deze ondertekenen.
2. Dit protocol is onderdeel van de dienstverleningsovereenkomst en zal gelden voor zolang deze overeenkomst duurt.
3. Na beëindiging van de dienstverleningsovereenkomst zullen de lopende verplichtingen, zoals het melden van Datalekken waarbij Persoonsgegevens van Partijen zijn betrokken en de plicht tot geheimhouding blijven voortduren.

Artikel 3 – Verantwoordelijkheid verwerkingsverantwoordelijke

Partijen conformeren zich aan de verplichting krachtens artikel 24 AVG, om passende en effectieve maatregelen te nemen om naleving van de AVG te borgen. Hierbij moeten Partijen aan kunnen tonen dat elke verwerkingsactiviteit past binnen de AVG.

Artikel 4 - Verwerken Persoonsgegevens

1. Partijen conformeren zich bij het verwerken van Persoonsgegevens aan de wet. De gegevens worden verwerkt op een behoorlijke, zorgvuldige en transparante wijze, als bedoeld in artikel 5 en 6 van de AVG.
2. Wanneer de dienstverlener andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens, sluit deze krachtens artikel 28 AVG met de verwerker een verwerkersovereenkomst.
3. Wanneer Partijen een verzoek van een Betrokkene ontvangen ten aanzien van het uitoefenen van zijn of haar rechten, zullen Partijen conform artikel 15 t/m 20 AVG, zorgen dat de Betrokkene zijn of haar rechten effectief kan uitoefenen. Deze rechten bestaan uit een verzoek om inzage, correctie, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.

Artikel 5 - Bewaartermijn gegevens

1. Voor de persoonsgegevens geldt een wettelijk bewaartermijn van 7 jaar.
2. Vernietiging van persoonsgegevens geschiedt met inachtneming van de Archiefwet.

Artikel 6 – Datalekken

1. In geval van een ontdekking van een mogelijk Datalek zullen Partijen elkaar hierover informeren binnen 24 uur overeenkomstig de procedure zoals die is opgenomen in Bijlage A.
2. Partijen zullen elkaar op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek, ook zullen Partijen de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan elkaar.
3. Partijen doen elk voor dat deel waar zij verantwoordelijk voor zijn de melding van een Datalek bij de Toezichthouder. Hetzelfde geldt voor de melding aan de Betrokkenen.

4. Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

Artikel 7 - Informatie-uitwisseling

Gegevens over cliënten worden alleen maar uitgewisseld door daartoe bevoegde personen van de SDD en Matchingunit. Voor zover dat gaat per e-mailverkeer worden daarvoor nooit privé-emailadressen gebruikt.

Artikel 8 – Aansprakelijkheid

Krachtens artikel 82 AVG is iedere verwerkingsverantwoordelijke in beginsel hoofdelijk aansprakelijk voor alle schade (waarbij iedere verwerkingsverantwoordelijke aansprakelijk is voor dat deel waarvoor zij aansprakelijk kan worden gesteld), ongeacht of die door hemzelf of door een verwerker is veroorzaakt. Geen aansprakelijkheid bestaat in geval van overmacht.

Vastgesteld en ondertekend te op

Namens de gemeente

Namens(naam contractpartner)

(Naam/functie).....

(Naam/functie).....

Bijlage A: Proces rondom het melden van Datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?

Een Datalek is een beveiligingsincident waarbij Persoonsgegevens, die de ene verantwoordelijke namens de andere verantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Elke verantwoordelijke dient voor het deel waar hij/zij verantwoordelijk voor is een melding te maken bij de Toezichthoudende autoriteit wanneer er sprake is van een beveiligingsincident. Het gaat om gegevens die te koppelen zijn aan personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens:

- De website met login-gegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT-systeem.
- Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

Wat te doen bij twijfel?

Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware zoals een IMEI-nummer, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits)fraude mee kan worden gepleegd, zoals een Burgerservicenummer?
- Zijn er grote hoeveelheden Persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de Persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met:

privacySDD@rechtsteden.nl.

Waar meld je het beveiligingsincident?

Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met: privacySDD@rechtsteden.nl.

Geef in je e-mail beantwoording op de onderstaande vragen

De onderstaande vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt wanneer er van het Datalek een melding gemaakt moet worden. Gaarne de vragen zo volledig mogelijk beantwoorden:

1. Geef een samenvatting van het beveiligingslek/beveiligingsincident/Datalek: wat is er gebeurd?
Vermeld hier ook de naam van het betrokken systeem.
2. Welke typen Persoonsgegevens zijn betrokken bij het beveiligingsincident?
Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. Van hoeveel personen zijn de Persoonsgegevens betrokken bij het beveiligingsincident?
Geef a.u.b. een minimum en maximum aantal personen.
4. Omschrijving groep personen om wiens gegevens het gaat.
Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van kwetsbare groepen personen, zoals kinderen.
5. Zijn de contactgegevens van de betrokken personen bekend?
Het kan zijn dat Betrokkenen geïnformeerd moeten worden over het Datalek, kunnen we deze personen in dat geval bereiken?
6. Wat is de oorzaak (root cause) van het beveiligingsincident?
Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?
Geef dit a.u.b. zo specifiek mogelijk aan.