DATA PRO CREATED BY NEDERLAND ICT

DATA PRO CODE

Versie april 2019

Voor de digitale economie

NEDERLAND ICT

DATA PRO CODE IN HET KORT

De Data Pro Code is een nadere uitwerking van de verplichtingen voor data processors (verwerkers) op grond van artikel 28 Avg. De Data Pro Code is van toepassing op verwerkingen in Nederland. De Data Pro Code geeft concrete gedragsregels voor verwerkers. De kern daarvan vormen de informatieplichten voor de data processor en de verantwoording door middel van toezicht.

Om te voldoen aan de informatieplichten vraagt de Data Pro Code om het invullen van een Data Pro Statement. In het Data Pro Statement informeren data processors op welke wijze zij concreet invulling hebben gegeven aan de Avg. Het Data Pro Statement vormt tezamen met de Standaardclausules voor verwerkingen een verwerkersovereenkomst.

De Data Processor die aantoonbaar in voldoende mate voldoet aan het gestelde in de Data Pro Code, wordt opgenomen in het Data Pro register. Een Data Processor die is geregistreerd, onderwerpt zich aan extern toezicht. Een Data Processor die niet, of niet langer, in voldoende mate voldoet aan het gestelde in de Data Pro Code, wordt verwijderd uit het Data Pro register. De Data Pro Code ligt momenteel ter goedkeuring bij de Autoriteit Persoonsgegevens.

DE DATA PRO CODE

BIJLAGEN:

DATA PRO CODE

I. INFORMATIEVERPLICHTINGEN – DATA PRO STATEMENT

1. De data processor informeert zijn opdrachtgever over de door hem getroffen beveiligingsmaatregelen ten aanzien van zijn dienst of product op zodanige wijze dat een opdrachtgever zelf in staat is een beoordeling te maken of deze voldoende zijn, gezien het door de opdrachtgever voorgenomen gebruik van de dienst of het product en daarmee mogelijke verwerking van persoonsgegevens. Data processor verwoordt dit in een *Data Pro Statement*.

1. De data processor heeft een 'Data Pro Statement' gepubliceerd of deze is opgenomen in de verwerkersovereenkomst.
2. In het Data Pro Statement is ten minste opgenomen:
    - het door de data processor gekozen information security management systeem, de beveiligingsnorm(en) of -standaard;
    - de – indien van toepassing –certificering(en) van de data processor;
    - of en welke (sub)data processors door de data processor worden ingezet;
    - op welke wijze gedurende de looptijd van de overeenkomst de persoonsgegevens van opdrachtgever verwijderd kunnen worden;
    - de bewaartermijn, indien wordt afgeweken van een vernietigingstermijn van 3 maanden;
    - de contactgegevens van de contactpersoon voor dataprotectie binnen de organisatie van de data processor.
3. In het Data Pro Statement informeert de data processor tenminste over de volgende beveiligingsmaatregelen:
    - pseudonimisering en versleuteling van persoonsgegevens;
    - het vermogen om op een permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
    - het vermogen om bij een incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen (back-ups, redundantie).

2. De data processor maakt in zijn verwerkersovereenkomst gebruik van de bij de Data Pro Code behorende Standaardclausules voor verwerkingen, of een daarmee vergelijkbare verwerkersovereenkomst.

1. Data processor houdt in zijn contractadministratie bij of de Standaardclausules voor verwerkingen van toepassing zijn.
2. Data processor houdt in zijn contractadministratie bij of een andere verwerkersovereenkomst of standaardclausules van toepassing zijn.

3. **De data processor informeert zijn opdrachtgever welke processen en procedures hij heeft ingericht waarmee de opdrachtgever, die controller is, gehoor kan geven aan de rechten van data subjects.**

    1. De data processor informeert zijn opdrachtgever over de mogelijkheden van data subjects om hun rechten te kunnen uitoefenen, waaronder hun recht op inzage, correctie, verzet en vergetelheid, in relatie tot de dienstverlening van de data processor aan zijn opdrachtgever, bijvoorbeeld in het Data Pro Statement.

4. **Indien de data processor in zijn organisatie een datalek ontdekt, zal de data processor zijn opdrachtgever daarvan zo snel mogelijk op de hoogte stellen, zodat de controller kan voldoen aan zijn wettelijke verplichting binnen 72 uur nadat hij er kennis van heeft genomen te melden bij de Autoriteit Persoonsgegevens of de betrokken data subjects. Wel of niet melden blijft de verantwoordelijkheid van de controller.**

    1. De data processor zal de opdrachtgever of de controller desgewenst ondersteunen bij het meldproces.
    2. De data processor levert bij een datalek de benodigde informatie en ten minste:
        - een omschrijving van het incident, aard van de inbreuk, aard van de persoonsgegevens c.q. categorieën van betrokken data subjects, schatting van het aantal betrokken data subjects en mogelijke betrokken databases, indicatie wanneer incident heeft plaatsgevonden (*wat is er gebeurd?*);
        - contactgegevens contactpersoon (*waar kan de controller met vragen terecht?*);
        - mogelijke gevolgen (*wat kan er gebeuren, waar moet de controller, dan wel het data subject, op bedacht zijn, wijzen op de mogelijkheden van identiteitsfraude als gegevens als BSN nummers, inlog en wachtwoordgegevens, paspoort kopieën mogelijk in verkeerde handen terecht zijn gekomen*);
        - genomen maatregelen (*wat heeft de data processor gedaan om eventuele schade te beperken of dit in de toekomst te voorkomen?*);
        - te nemen maatregelen door de controller dan wel betrokken data subjects (*wat kunnen betrokken data subjects zelf doen, bijvoorbeeld "houd mail in de gaten, wijzig wachtwoorden");*
        - de data processor blijft de opdrachtgever op de hoogte houden van verdere ontwikkelingen.

5. **De data processor toetst en evalueert regelmatig zijn dataprotectiebeleid en genomen beveiligingsmaatregelen en past deze waar nodig aan.**

    1. Bij relevante ontwikkelingen informeert Data processor zijn opdrachtgever over de door hem uitgevoerde (interne) controles, zoals door:

- wel of niet verkregen hercertificering, bijvoorbeeld door een verwijzing naar een openbaar toegankelijke register;
- informatie over periodieke externe controles, zoals audits of beschikbaar stellen van een Third Party Memorandum (TPM's);
- informatie, of relevante onderdelen, uit een assurance rapport met conclusies over de bevindingen van de auditor;
- eigen controles of eigen mededelingen door de data processor.

II. TOETSING EN TOEZICHT

1. Toetsing en toezicht

1. Er is een onafhankelijke toezichthouder op de Data Pro Code, de Data Pro Toezichthouder.
2. De Data Pro Toezichthouder draagt zorg voor toezicht op het toetsingsproces en op naleving van de Data Pro Code door data processor.
3. De data processor die de Data Pro Code toepast zal zich onafhankelijk laten toetsen.
4. Toetsing bestaat uit periodieke toetsing en additionele toetsingen. Periodieke toetsingen vinden jaarlijks plaats. Additionele toetsingen vinden plaats op ad random basis en kunnen plaatsvinden naar aanleiding van een klacht of signaal.
5. Bij toetsing met een voldoende resultaat wordt de data processor door de Data Pro Toezichthouder opgenomen in het openbaar toegankelijk Data Pro register.
6. Een geregistreerde data processor verkrijgt een gebruiksrecht om het Data Pro Certificate te gebruiken waarmee hij aantoont dat hij zich houdt aan het gestelde in de Data Pro Code.

2. Data Pro register

1. De Data Pro Toezichthouder beheert het Data Pro register en maakt het register openbaar.
2. De Data Pro Toezichthouder besluit tot opname van een data processor in het register.
3. Bij een onvoldoende resultaat na toetsing, of indien een klacht, wet of openbare orde daartoe aanleiding geven, zal de Data Pro Toezichthouder besluiten tot het verwijderen van de betreffende data processor uit het Data Pro register. De Data Pro Toezicht-houder kan besluiten verwijdering uit het Data Pro register openbaar te maken.

3. Klachten

1. De Data Pro Toezichthouder draagt zorg voor een klachtenprocedure.

III. WERKING EN AANPASSING DATA PRO CODE

1. Werking

1. Deze code is in werking vanaf [datum goedkeuring AP].

2. Data Pro Code College en aanpassing Data Pro Code

1. Er is een Data Pro Code College.
2. Deze code wordt regelmatig geëvalueerd, tenminste eens per twee jaar door het Data Pro Code College.
3. Wijzigingen op de code worden eerst vastgesteld door het Data Pro Code College.
4. Eventuele wijzigingen in de code zullen opnieuw aan de Autoriteit Persoonsgegevens worden voorgelegd ter goedkeuring.
5. De Data Pro Toezichthouder zal van een voornemen tot eventuele wijzigingen van de code vooraf kennis geven aan alle geregistreerde data processors opdat zij voldoende tijd hebben te (blijven) voldoen aan de recentste versie van de code.

BIJLAGE 1: VERWERKERSOVEREENKOMST

- Ben je lid van Nederland ICT? Download dan de Standaard verwerkersovereenkomst hier in MijnNederlandICT.

- Ben je geen lid, dan kun je de Standaard verwerkersovereenkomst hier bestellen. Op deze pagina vind je ook een inkijkexemplaar.

BIJLAGE 2: UITGANGSPUNTEN PRIVACYBELEID EN DATA PRO STATEMENT

De Data Pro Code vraagt om het invullen van een Data Pro Statement. Om tot een evenwichtige en toetsbare invulling van het Data Pro Statement te komen, zal een data processor een onderliggend privacybeleid moeten hebben. Dat privacybeleid kan hij nader invullen aan de hand van onderstaande algemene uitgangspunten. De uitgangspunten dwingen tot bewuste keuzes in de omgang met persoonsgegevens en stimuleren een veilige en verantwoorde omgang met gegevens.

UITGANGSPUNT 1 - OMSCHRIJVING EN BEOORDELING DIENSTVERLENING

UITGANGSPUNT 2 - BELEID EN GOVERNANCE

UITGANGSPUNT 3 - ORGANISATIE EN MIDDELEN

UITGANGSPUNT 4 - LIMITERING GEBRUIK

UITGANGSPUNT 5 - BEVEILIGING VAN PERSOONSGEGEVENS

TOELICHTING OP DE UITGANGSPUNTEN

UITGANGSPUNT 1 - OMSCHRIJVING EN BEOORDELING DIENSTVERLENING

De door de data processor aangeboden diensten of producten zijn door de data processor omschreven en beoordeeld, rekening houdend met de markt waarin hij opereert, het door de data processor beoogd gebruik van zijn dienst of product en daarmee de binnen of met zijn dienst of product verwachte aard van de te verwerken data en het aantal te verwerken data subjects.

UITGANGSPUNT 2 - BELEID EN GOVERNANCE

De data processor heeft een gedocumenteerd beleid voor dataprotectie, waaronder een datalekprocedure.

UITGANGSPUNT 3 - ORGANISATIE EN MIDDELEN

De data processor heeft zijn dataverwerking in kaart gebracht.

UITGANGSPUNT 4 - LIMITERING GEBRUIK

De data processor heeft geborgd dat de verkregen persoonsgegevens van zijn opdrachtgever uitsluitend worden verwerkt voor de verlening van zijn diensten aan die opdrachtgever.

UITGANGSPUNT 5 - BEVEILIGING VAN PERSOONSGEGEVENS

5.1 De data processor heeft passende technische en organisatorische maatregelen getroffen om een beveiligingsniveau voor persoonsgegevens te waarborgen dat is

afgestemd op het risico dat is verbonden aan het door de data processor beoogde gebruik van zijn dienst of product.

5.2 **Bij de beoordeling van het passende beveiligingsniveau houdt de data processor rekening met de verwerkingsrisico's verbonden aan zijn dienst of product, met name ten aanzien van mogelijke gevolgen van vernietiging, verlies, wijziging of ongeoorloofde toegang tot persoonsgegevens binnen of via zijn dienst of product, hetzij per ongeluk hetzij onrechtmatig.**

5.3 **De data processor hanteert een information security management systeem, beveiligingsnorm of -standaard, waarbij is voorzien in een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de getroffen beveiligingsmaatregelen voor persoonsgegevens door de data processor (*plan, do, check, act*).**

TOELICHTING

Hieronder wordt voor ieder uitgangspunt uitgewerkt wat eronder wordt verstaan en welke uitgangspunten of best practices daarbij nagestreefd worden.

BIJ UITGANGSPUNT 1 - OMSCHRIJVING EN BEOORDELING DIENSTVERLENING

Een goede omschrijving van de diensten is de basis voor goede informatievoorziening en geeft de basis om tot een juiste risicoafweging te komen, waarop de gekozen beveiligingsmaatregelen gebaseerd moeten zijn. Het is daarom van belang om de volgende onderdelen intern uit te werken en daarin heldere keuzes te maken:

1. De data processor heeft het beoogd gebruik van zijn dienst of product helder omschreven.
2. De data processor heeft de verwachte aard van de te verwerken persoonsgegevens in of met zijn dienst of product omschreven (*ten minste aangeven: wel/niet bijzondere persoonsgegevens*).
3. De data processor heeft de markt waarin hij opereert beoordeeld en heeft zijn dienst of producten op die beoordeling afgestemd (privacy by design), daarbij rekening houdend met:
    - het aantal data-elementen per data subject (*dataminimalisatie*);
    - het verwachte aantal te verwerken data subjects (*minder of meer dan 100.000 betrokkenen*);
    - het beoogde gebruik van zijn dienst of product (*ten minste aangeven: is dienst of product wel/niet cruciaal in de bedrijfsvoering van een opdrachtgever; Deze beoordeling vormt een Data Protectie Impact Assessment (DPIA) op de dienstverlening*).

BIJ UITGANGSPUNT 2 - BELEID EN GOVERNANCE

Compliance met de Avg vergt een intern privacybeleid. Onderstaande onderwerpen moeten daarbij aandacht krijgen:

1. De data processor heeft zijn keuze voor het niveau van door hem te treffen beveiligingsmaatregelen gedocumenteerd (*visie op dataprotectie*).
2. Bij de inrichting van zijn eigen dienst of product heeft de data processor maatregelen genomen om verwerking van niet-noodzakelijke persoonsgegevens bij het gebruik van zijn dienst of product te voorkomen (*privacy by design*).
3. De data processor weet in geval van een datalek hoe te handelen (*datalekprotocol*).
4. De data processor heeft een contactpersoon aangewezen voor dataprotectie die kennis heeft (of verkrijgt door opleiding) van dataprotectie.

BIJ UITGANGSPUNT 3 - ORGANISATIE EN MIDDELEN

Voor de invulling van de informatieplichten en om een goede risicobeoordeling te kunnen geven, is inventarisatie van zowel toeleveranciers als klanten van groot belang. Denk daarbij aan de volgende onderdelen:

1. De data processor heeft de door hem gebruikte middelen en door hem ingezette leveranciers in kaart gebracht (*er is een overzicht van middelen en leveranciers ((sub)data processors) die nodig zijn voor zijn dienstverlening*).
2. De data processor heeft beoordeeld of de door hem gebruikte middelen en door hem ingezette leveranciers ((sub)data processors) voldoende waarborgen bieden ten aanzien van dataprotectie.
3. De data processor heeft een accurate contractadministratie (*kan daarmee voldoen aan de verwerkingsregisterplicht*).

BIJ UITGANGSPUNT 4 - LIMITERING GEBRUIK

Dataminimalisatie en limitering van gebruik van gegevens is verankerd in de Avg. Klanten zullen van data processors inzicht willen hoe dit geregeld is. Best practices hierbij zijn:

1. Persoonsgegevens van een opdrachtgever worden alleen gebruikt voor het uitvoeren van de overeenkomst met die opdrachtgever.
2. Persoonsgegevens van een opdrachtgever worden door de data processor gescheiden van persoonsgegevens van andere opdrachtgevers.
3. Medewerkers van de data processor is geheimhouding opgelegd van persoonsgegevens van een opdrachtgever.
4. De data processor zal persoonsgegevens na het einde van de overeenkomst met de opdrachtgever in een machineleesbaar formaat aan de opdrachtgever ter beschikking stellen indien dit is overeengekomen.
5. De data processor borgt dat persoonsgegevens van een opdrachtgever na het einde van de overeenkomst met die opdrachtgever of na voltooiing van een opdracht voor die opdrachtgever binnen drie maanden na het einde ervan worden verwijderd op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (*render inaccessable*).

BIJ UITGANGSPUNT 5 - BEVEILIGING VAN PERSOONSGEGEVENS

Misschien wel de belangrijkste verplichting van een data processor is het zorgen voor een passende beveiliging van de persoonsgegevens die hij verwerkt. In een snel veranderende wereld vergt een goed beveiligingsbeleid ook doorgaand onderhoud. Om een afweging te kunnen maken welke maatregelen passend zijn en hoe de beveiliging doorgaand kan worden bijgehouden, helpt het om de volgenden uitgangspunten te hanteren:

1. Data processor maakt gebruik van een in de branche erkend Information Security Management Systeem (ISMS), technische beveiligingsstandaard of checklist.
2. Data processor kiest aan de hand daarvan de beveiligingsmaatregelen die specifiek voor zijn product of dienst geschikt zijn.
3. De data processor heeft de volgende beveiligingsmaatregelen meegewogen in zijn keuzes :
    - pseudonimisering en versleuteling van persoonsgegevens;
    - het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
    - het vermogen om bij een incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen (*back ups, redundantie*).
4. Bij de beoordeling van een passend beveiligingsniveau voor zijn dienst of product houdt de data processor rekening met:
    - de stand van de techniek;
    - de uitvoeringskosten;
    - de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van individuele data subjects;
    - de markt waarin hij opereert;
    - het aantal data-elementen per data subject en de verwachte aard van de te verwerken data (*ten minsten aangeven: wel/niet bijzondere persoonsgegevens*);
    - het verwachte aantal van te verwerken data subjects (*ten minste aangeven: minder of meer dan 100.000 betrokkenen*);
    - het beoogde gebruik van zijn dienstverlening door een opdrachtgever (*ten minste aangeven: is de dienstverlening wel/niet cruciaal in de bedrijfsvoering van een opdrachtgever*).
5. Data processor legt de keuzes en genomen maatregelen vast in zijn dataprotectiebeleid.
6. Data processor legt de relevante delen van de beveiligingsmaatregelen vast in zijn Data Pro Statement, of ander document waarvan opdrachtgever kennis kan nemen.
7. Data processor doorloopt de opgestelde procedures van zijn dataprotectiebeleid zo vaak als nodig doch ten minste eens in de 12 maanden en in lijn met het gehanteerde ISMS.
8. Data processor zal de aanbevolen verbetermaatregelen na een controle doorvoeren voor zover redelijkerwijze van hem mag worden verwacht. Data processor documenteert de aanpassingen die volgen uit de doorlopen procedure in het dataprotectiebeleid.