DATA PRO CREATED BY NEDERLAND ICT

DATA PRO CODE

Versie januari 2018

Voor de digitale economie

NEDERLAND ICT

DE CODE IN HET KORT

Acht principes voor professionele dataprotectie.

Een concrete invulling van actuele privacy- en securityregels.

Gericht op kleine en middelgrote data processors.

INHOUD

VOORWOORD

De ICT-sector is heel divers, maar één ding dat de meeste ICT-bedrijven gemeen hebben is dat zij data verzamelen, bewerken en bewaren in opdracht van hun klanten. Voor deze rol van 'data processor' bestaan wettelijke richtlijnen op het gebied van privacy en security, in het bijzonder de nieuwe Europese verordening gegevensbescherming (Avg/GDPR). Om bedrijven te helpen aan deze regels te voldoen, heeft Nederland ICT de Data Pro Code ontwikkeld.

De Data Pro Code is voor data processors een instrument om op een veilige en privacy-vriendelijke manier met data om te gaan. De acht principes uit de code zijn een concrete invulling van actuele wetgeving. De code biedt ICT-bedrijven kaders en houvast voor de verwerking van gegevens en zorgt voor openheid en verantwoording richting hun klanten.

Nederland ICT heeft de code ontwikkeld in samenwerking met leden. Tijdens het ontwikkelen van de code hebben we expliciet de praktijk van kleine tot middelgrote ICT-ondernemers als uitgangspunt genomen. Het moet voor elk ICT-bedrijf, van klein tot groot, haalbaar zijn om de code toe te passen.

Data processors die de Data Pro Code toepassen laten zien dat zij staan voor een professionele omgang met de persoonsgegevens die aan hen worden toevertrouwd. Voor klanten en ketenpartners biedt de code duidelijkheid en transparantie over wat ze van ICT-bedrijven mogen verwachten.

Ik ben ervan overtuigd dat de Data Pro Code hiermee een solide basis is voor verdere professionalisering van de sector en wederzijds vertrouwen in de markt.

Lotte de Bruijn, directeur Nederland ICT

UITGANGSPUNTEN

Met de Data Pro Code neemt Nederland ICT haar verantwoordelijkheid als brancheverenigingen van de ICT-sector

De Europese privacyregels (Avg, of in het Engels: GDPR) bieden in grote lijnen principes voor de omgang met persoonsgegevens. De vertaling en invulling van deze principes verschilt sterk per branche of zelfs per bedrijf. In de Avg wordt daarom expliciet verwezen naar de rol van brancheverenigingen bij het implementeren van de Avg.
Met het ontwikkelen van de Data Pro Code geeft Nederland ICT invulling aan deze rol. We nemen bovendien onze verantwoordelijkheid om de sector verder te professionaliseren op het gebied van privacy en security. Met de Data Pro Code willen we duidelijkheid en transparantie in de markt bevorderen en daarmee het vertrouwen in de ICT-sector vergroten.

De Data Pro Code is voor verwerkers

Bedrijven die voor hun klanten data verzamelen, bewerken en bewaren zijn onder de Avg/GDPR 'verwerkers', of – in het Engels – 'data processors'. De Data Pro Code is ontwikkeld met deze juridische rol als uitgangspunt. Door de code toe te passen geeft een bedrijf op een professionele manier invulling aan zijn rol als data processor. De term Data Pro verwijst naar beide aspecten van privacy: juridisch (data processor) en bedrijfsmatig (data professional).

De Data Pro Code is een concrete invulling van de Avg

Door toepassing van deze code kunnen data professionals aan de buitenwereld tonen dat zij:

- hebben nagedacht over omgang met persoonsgegevens;
- hun organisatie hebben ingericht om een veilige omgang met persoonsgegevens van een opdrachtgever te borgen.

Deze code geeft daarmee een praktische en nadere invulling aan de vereisten die zijn opgenomen voor data processors in de Avg/GDPR.

De Data Pro Code is gebaseerd op vrijwillige, normatieve principes en best practices

De Data Pro Code komt niet in de plaats van de eigen verantwoordelijkheid van organisaties. De code biedt een normatief kader voor data processors voor de bescherming van persoonsgegevens ('dataprotectie'). Daarom kent de Data Pro Code algemene principes. De principes in de code vinden hun vertaling in praktijkaanbevelingen, oftewel 'best practices'. Deze kun je op verschillende manieren lezen: 'zo hoort het' of 'dit zijn goede praktijkvoorbeelden'.

Wie, vanwege het karakter of de omvang van zijn organisatie, wil afwijken van de code is daarin vrij. In het kader van de verantwoording en de transparantie is het dan wél van belang dat te kunnen uitleggen. Vandaar het principe: ‘pas toe of leg uit’.

De Data Pro Code is voor alle data professionals, van micro tot groot

Het uitganspunt bij het ontwikkelen van de code was de praktijk van kleine en micro-organisaties, zoals die zijn genoemd in de Avg. Kleine organisaties zijn organisaties met minder dan 50 werknemers, micro-organisaties hebben minder dan 10 werknemers. Dat betekent niet dat de code niet van toepassing is op grotere organisaties. Iedere dienstverlener die zichzelf als een data professional beschouwt, kan de Data Pro Code toepassen. Groot of klein.

De Data Pro Code biedt duidelijkheid en transparantie

De organisaties die deze Data Pro Code toepassen, informeren hun opdrachtgevers hoe zij dataprotectie hebben geborgd in hun organisatie. Daarnaast informeren zij waar hun diensten of producten geschikt voor zijn, als het gaat om een beoordeling van bescherming van persoonsgegevens. Daarmee kunnen opdrachtgevers, of dat nu controllers of data processors zijn, zelf beoordelen of en op welke wijze zij gebruik willen maken van de producten en/of diensten van een organisatie die in opdracht van hen persoonsgegevens zullen verwerken. De Data Pro Code toepassen betekent dat je vastlegt én uitlegt hoe je de bescherming van persoonsgegevens geregeld hebt.

DE DATA PRO CODE

PRINCIPE 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.

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 (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 (meer dan 100.000 betrokkenen?);
    - het beoogde gebruik van zijn dienst of product (is zijn dienst of product wel/niet cruciaal in de bedrijfsvoering van een opdrachtgever?; *Data Protectie Impact Assessment (DPIA) op de dienstverlening*).

PRINCIPE 2 - BELEID EN GOVERNANCE

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

1. De data processor heeft zijn keuze voor het niveau van door hem te treffen beveiligingsmaatregelen gedocumenteerd (*visie en missie 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.

PRINCIPE 3 - ORGANISATIE EN MIDDELEN

De data processor heeft zijn dataverwerking in kaart gebracht.

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*).

PRINCIPE 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.

1. Persoonsgegevens van een opdrachtgever worden door de data processor gescheiden van persoonsgegevens van andere opdrachtgevers.
2. Medewerkers van de data processor hebben een verplichting tot geheimhouding van persoonsgegevens van een opdrachtgever.
3. De data processor kan persoonsgegevens na het einde van de overeenkomst met de opdrachtgever in een machineleesbaar formaat aan de opdrachtgever ter beschikking stellen indien dit is overeengekomen.
4. 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*).

PRINCIPE 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.

1. Data processor kan gebruik maken van een in de branche erkende technische beveiligingsstandaard of checklist.
2. Data processor kiest een eigen lijst met beveiligingsmaatregelen die specifiek voor zijn product of dienst geschikt zijn.

3. De data processor heeft de volgende beveiligingsmaatregelen betrokken in zijn keuzes voor de beveiligingsnorm of standaard:
    - 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 persoonsgegeven tijdig te herstellen (back ups, redundantie).

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.

1. 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 en de verwachte aard van de te verwerken data (wel/niet bijzondere persoonsgegevens?);
    - het verwachte aantal van te verwerken data subjects (meer dan 100.000 betrokkenen?);
    - het beoogde gebruik van zijn dienstverlening door een opdrachtgever (is de dienstverlening wel/niet cruciaal in de bedrijfsvoering van een opdrachtgever?).

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*).

1. Het door de data processor gekozen information security management systeem is vastgelegd in zijn dataprotectiebeleid.

2. De data processor kan zich aansluiten bij of conformeren aan één of meer in de branche erkende beveiligingsnormen.

PRINCIPE 6 - INFORMATIEVERPLICHTINGEN – DATA PROCESSOR STATEMENT

6.1 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 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 tenminste 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 de data processor persoonsgegevens buiten de Europese Economische Ruimte (EER) verwerkt of laat verwerken;
    - of en welke (sub)data processors door de data processor worden ingezet;
    - de bewaartermijn, indien wordt afgeweken van de vernietigingstermijn van 3 maanden in 4.4;
    - 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).

6.2 De data processor maakt in zijn verwerkersovereenkomst in beginsel gebruik van de bij de Data Pro Code behorende Standaardclausules voor verwerkingen.

1. De data processor houdt in zijn contractadministratie bij of de Standaardclausules voor verwerkingen van toepassing zijn.

6.3 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 tenminste:
    - 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.

PRINCIPE 7 - RECHTEN VAN DATA SUBJECTS

De data processor informeert zijn opdrachtgever of hij processen en procedures 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.

PRINCIPE 8 - VERANTWOORDING (ACCOUNTABILITY)

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

1. De data processor die de Data Pro Code toepast kan zich onafhankelijk laten toetsen. Bij een voldoende resultaat kan de data processor het Data Pro Certificate gebruiken, waarmee hij kan aantonen dat hij zich houdt aan de Data Pro Code.
2. De gecertificeerde data processor wordt opgenomen in een openbaar toegankelijk register.
3. De gecertificeerde data processor kan tussentijds worden getoetst (op basis van steekproef of na klachten) en zal zich jaarlijks (laten) hertoetsen.
4. Het gebruiksrecht op het Data Pro Certificate kan worden ingetrokken door de certificerende instantie na klachten of na onderzoek. Het gebruiksrecht op het certificaat door de data processor vervalt na een onvoldoende resultaat bij een hertoetsing.
5. De data processor informeert zijn opdrachtgever periodiek over de door hem uitgevoerde (interne) controles, zoals door:
    - wel of niet verkregen hercertificering, bijvoorbeeld door een verwijzing naar het 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.
6. De data processor zal de aanbevolen verbetermaatregelen na een controle doorvoeren voor zover redelijkerwijze van hem mag worden verwacht.

VERKLARENDE WOORDENLIJST

	Gedefinieerd in Avg/GDPR als:	
Controller	*Avg: "verwerkings-verantwoordelijke"* *GDPR: "controller"*	Conform Avg: *"een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt"*
Data processor	*Avg: "verwerker"* *GDPR: "processor"*	Conform Avg: *"een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt".*
Dataprotectie	*Avg: "gegevensbescherming"* *GDPR: "data protection"*	Bescherming van persoonsgegevens.
Data subject	*Avg: "betrokkene"* *GDPR: "data subject"*	Conform Avg: *"een geïdentificeerde of identificeerbare natuurlijke persoon".*
Opdrachtgever		De opdrachtgever kan zowel een controller als een andere data processor zijn in wiens opdracht de data processor persoonsgegevens verwerkt.
Persoonsgegevens	*Avg: "persoonsgegevens"* *GDPR: "personal data"*	Conform Avg: "*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon".*
Standaardclausules	*Avg:"standaard contract-bepalingen"* *GDPR: "standard contractual clauses"*	De standaard contractbepalingen als bedoeld in artikel 28 lid 8 Avg.

Verwerking		Conform Avg: *"een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens".*
Verwerkers-overeenkomst		De overeenkomst waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van data subjects, en de rechten en verplichtingen van de controller worden omschreven; zoals omschreven in artikel 28 lid 3 Avg.