Wat maakt een goede FG?

Deel 2: Risicosturing

Sergej Katus[1]

Deze tweede blog in de reeks 'Wat maakt een goede FG?' gaat over risicosturing. Dat klinkt paniekerig, maar juist een goed FG weet risico om te keren in rust en houvast. We zien hoe onmisbaar de objectieve beoordeling is die in de AVG wordt voorgeschreven – om er vervolgens achter te komen dat je zonder de Schaal van Erg nooit objectief genoeg kunt zijn. Dus; hoe erg is bijvoorbeeld een smoelenboek? En hoeveel prioriteit verdient zoiets? Gelukkig is er altijd nog de PIA om dat grondig uit te zoeken. En lang leve de Schaal van Erg als je de FG van een verwerker bent.

Deze blog voor functionarissen voor gegevensbescherming (data protection officers) is de tweede in een korte reeks. De eerste blog ging over de juiste persoon in de juiste setting. Ook werden tien vragen aangereikt om te checken of je setting als FG genoeg klopt. In deze blog gaan we dieper in op je missie – we noemden dit het FG-kompas – volgens artikel 39.2 AVG:

'De FG houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.'

We zagen dat wie zich door artikel 39.2 laat leiden, focust op échte oplossingen voor échte problemen. Je maakt problemen niet groter of kleiner dan ze zijn en weet werkelijke oplossingen te onderscheiden van nep-oplossingen.

In deze blog werken we dat nader uit aan de hand van het risicobegrip in de AVG, zoals dit ook terugkeert in 39.2.

Risico is *key*

Als je telt hoe vaak het woord 'risico' voorkomt in de AVG (ruim 70 keer), zou je verwachten dat de wetgever wel de moeite had genomen om 'risico' op te nemen in de definities van artikel 4. Maar nee. Dat is best gek wanneer je je realiseert het woord een sleutelrol heeft in kernartikelen 24 en 25 van de AVG. Artikel 24 stelt verwerkingsverantwoordelijken tot opdracht om het recht op bescherming van persoonsgegevens te waarborgen, door te sturen op (artikel 25) 'privacy by design'. Maar dan wel – daar heb je 'm – 'rekening houdend met de (…) qua ernst en waarschijnlijkheid uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen'. Wat ís dat?

Kennelijk is 'risico' *key*. Hierna komen we beslist nog terug op zowel de ernst en waarschijnlijkheid als de rechten en vrijheden voor personen. Maar laten we dat voor nu parkeren en even doorlezen in artikel 24 en 25, want wat daar vooral opvalt, is dat de wetgever de nadruk leggen op het nemen van *passende maatregelen*. Dat leidt tot de volgende logica: wie de risico's niet snapt, snapt ook de maatregelen niet die genomen moeten worden, laat staan dat je snapt wanneer ze ook echt passend zijn.

---

[1] mr S.H. Katus, CIPP/E CIPM FIP is functionaris voor gegevensbescherming en partner bij Privacy Management Partners.

Voor een goed FG is dat onbestaanbaar. Want jij bent degene die je organisatie moet leiden naar passende maatregelen, om er vervolgens op te letten dat je organisatie die maatregelen ook echt néémt. Het mag niet zo zijn dat ook jij in het duister tast.[2] Het geeft niet dat je niet ogenblikkelijk de risico's snapt. Sterker nog; dat kenmerkt je als goed FG. De vraag is vooral wat je er aan doet om wél aan die kennis te komen.

Rust en houvast

In ieder geval zijn er twee dingen die je vooral *niet* moet doen: (1) in alles en nog wat een risico zien voor de privacy; en (2) in alles en nog wat wijzen op het risico van boetes tot 20 miljoen. Want waarom zou je schrik willen aanjagen? In het beste geval resulteert dat in paniekvoetbal en verkramping – en daarom hoogstwaarschijnlijk juist in *niet*-passende oplossingen. Bovendien ondergraaf je je eigen positie – zeker als de boetes uitblijven. Want 'aan die onheilsprofeet hebben we niks'. Mensen nemen je niet meer serieus laten je links liggen.

Een goed FG creëert rust en houvast, en biedt inspiratie. Dat artikel 4 geen risicodefinitie bevat is voor jou geen enkel probleem, want je hebt meer dan genoeg aan overweging 76 AVG:

'De waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkene moeten worden bepaald onder verwijzing naar de aard, het toepassingsgebied, de context en de doeleinden van de verwerking. Het risico moet worden bepaald op basis van een objectieve beoordeling en vastgesteld moet worden of de verwerking gepaard gaat met een risico of een hoog risico.'

Hoe je precies rust en houvast creëert, is helemaal aan jou als professional. Maar misschien is het een goed idee om te beginnen met de vaststelling van een formele richtsnoer voor je organisatie ('FG-aanwijzing'). Hierin verduidelijk je hoe risico's AVG-conform moeten worden ingeschat, om ze daarna richting te bieden om veilig op die risico's in te spelen. Dat is althans wat de wetgever voorstelt in overweging 77 AVG.

Objectieve beoordeling

Wat je aanpak ook is – voor jou is een risico pas een risico als dat de uitkomst is van de objectieve beoordeling die in overweging 76 wordt genoemd. Zo'n beoordeling is uiteindelijk aan jou als wettelijk toezichthouder, maar je wilt in de eerste plaats dat je organisatie zelf zo bekwaam is om uit zichzelf de beoordeling goed te doen.

Waar het in de kern om gaat bij een objectieve beoordeling, is dat zowel de *ernst* als de *waarschijnlijkheid* van problemen met de gegevensverwerking op een evenwichtige wijze vast moeten komen te staan. Dat komt neer op het eerlijk uitzoeken van oorzaak en gevolg van problemen, zodat het reële (AVG-relevante) risico in beeld komt.[3]

- Om van ernst te kunnen spreken, moet de situatie in de eerste plaats te plaatsen zijn in de in de 'ernst-catalogus' van overweging 75.

- De waarschijnlijkheid neemt toe naarmate gegevensverwerking grootschaliger zijn en/of naar hun aard verhoogd risicogevoelig. Dat geldt in het bijzonder voor de gegevenstypen die in artikel 9 AVG, die in de wet daarom dan ook de 'bijzondere gegevenscategorieën' heten.

De factoren ernst en waarschijnlijkheid moeten tegen elkaar worden afgewogen om tot een risicobeoordeling te komen: is er sprake van een substantieel risico of moet het risico zelfs als hoog beoordeeld worden?[4]

---

[2] Of begin anders weer bij blog 1.
[3] Vgl. deze EDPB-post op LinkedIn over '*genuine* risks'.
[4] In feite gaat de AVG uit van de klassieke opvatting 'risico = kans x impact'.

Hoog risico is de reële kans op *ernstige* lichamelijke, materiële of immateriële schade voor een persoon, zo blijkt uit het eerste deel van overweging 75. Een substantieel risico is de reële kans op *aanzienlijk* economisch of maatschappelijk nadeel. Logischerwijs zit onder de risicogrens alle problematiek die niet aanzienlijk of ernstig genoeg is om als risico te worden aangemerkt (risico = klein/laag). Gemakshalve noemen we die categorie hierna de 'kleinigheden'.

To* meld *or not to* meld, *that's the question

De wetgever houdt dezelfde lijn aan bij de meldplicht datalekken volgens artikelen 33 en 34 AVG, waarbij je óók steeds een objectieve beoordeling zult moeten toepassen:

1. wanneer een incident voor personen een noemenswaardig risico inhoudt, is je organisatie gehouden om dit te melden aan de Autoriteit Persoonsgegevens;
2. wanneer zelfs sprake is van hoog risico voor personen, moeten ook zij worden geïnformeerd.

Kleinigheden hoeft je organisatie niet te melden,[1] volgt uit de tenzij-constructie in artikel 33. De achterliggende reden is dat je mensen niet met kleinigheden ongerust moet maken. Bovendien scheelt de ondergrens van risico je organisatie tijd en energie, en dat scheelt ook in de belasting van de AP als de centrale toezichthouder.

Belang of risico?

Terug naar je 39.2-aanpak. Als FG zul je in de omgang met risico's je niet alleen moeten laten leiden door risico's in de negatieve zin van het woord. Want als het goed is, heeft de gegevensverwerking op de een of andere manier vooral *nut*. En ook daarmee heb je naar behoren rekening te houden.

Neem bijvoorbeeld salarisuitbetaling. Dat is een en al verwerking van persoonsgegevens, tot het moment dat je contant geld in handen hebt. Het zet op het verkeerde been om voortdurend te denken in risico's – denk vooral in het belang van het feit dat iemand iedere maand netjes op tijd salaris ontvangt. Dat belang is aanzienlijk, en als salarisuitbetaling te lang uitblijft, kan het zelfs voor de persoon van vitaal belang worden dat de gegevensverwerking weer op gang komt, om er financieel gezien niet aan onderdoor te gaan. Het risico zit niet in de gegevensverwerking maar in de verstoring van het proces.

Daar komt nog bij dat we ook niet voorbij mogen gaan aan het organisatiebelang. Dat vloeit rechtstreeks voort uit overweging 4 AVG, in het bijzonder de zinsnede:

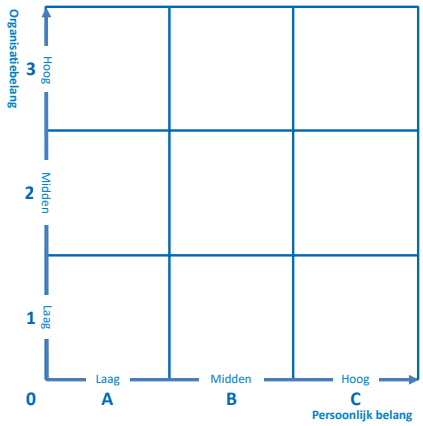
'Het recht op bescherming van persoonsgegevens heeft geen absolute gelding, maar moet worden beschouwd in relatie tot de functie ervan in de samenleving (...).'

Want waar blijft die relatie als je alleen maar oog hebt voor de belangen van personen? Het organisatiebelang is het bestuurlijk belang, bedrijfsbelang of, als we doorgaan op het voorbeeld van salariëring, het werkgeversbelang, bij verwerking van persoonsgegevens. Het gaat steeds om de context en het verwerkingsdoel waar voortdurend in de AVG op gewezen wordt – zie de overwegingen, artikel 5.1b, het gebruik van 'noodzaak' in artikel 6, artikelen 24-25 AVG en je missie als FG volgens 39.2.

Laten we blijven bij salariëring: gespiegeld is beloning voor prestatie net zozeer belangrijk (noodzakelijk) voor werkgevers. Daarom investeren ze ook (vaststelling van doel en middelen) in salariëringsoplossingen – hetzij in eigen huis, hetzij uitbesteed aan verwerkers. Als je exact wilt weten hoe groot het belang voor een werkgever is, zou je de *total cost of ownership* van het salariëringsproces kunnen uitrekenen (investeringskosten en beheerskosten, of de kosten van uitbesteding). Maar laten we het er hier op houden dat die kosten niet klein en niet hemelschrijend hoog zijn, maar iets daartussen in, dus ook aanzienlijk (substantieel).

De Schaal van Erg

Zo komen we op de Schaal van Erg, waarmee een goed FG voortdurend bezig is – bewust of onbewust – om invulling te geven aan de missie in 39.2. Het persoonlijk belang zet je af tegen de x-as. Het organisatiebelang zet je af tegen de y-as, en je beperkt je tot de indeling kleinigheid (laag), aanzienlijk/substantieel (midden), vitaal belang/ernstig (hoog). Door met coördinaten te werken, beschik je nu over een geschikter instrument voor objectieve beoordeling. Dat helpt je meteen bij het stellen van prioriteiten. Aan A1tjes besteedt je alleen tijd als je niets beters te doen hebt. Voor C3's breek je je vakantie af als dat risico zich manifesteert.



De Schaal van Erg laat zich voor van alles gebruiken en werkt prettig intuïtief. Gegevensverwerking voor salarisuitbetaling? B2. Een smoelenboek? A1. Gegevensverwerking in het kader van thuiszorg? C3 (tenminste; als de organisatie maatschappelijk opvalt en in de thuiszorgketen een sleutelrol speelt, terwijl er vitale persoonlijke belangen op het spel staan).

Het goede is ook dat iedere classificatie niet alleen getalsmatig veel verduidelijkt (vgl. een aardbeving met kracht van 3,4 op de schaal van Richter), maar ook meteen het aanknopingspunt biedt om de dialoog aan te gaan: 'Ik wil van een A1 best iets hogers maken, maar wat zijn daarvoor dan de argumenten?'. Zo helpt de Schaal van Erg ook om vast te stellen of en aan wie een datalek moet worden gemeld (de meldplicht gaat pas spelen bij incidenten vanaf B1). Of om beter te begrijpen wat grootschaligheid doet. Want, bijvoorbeeld, wanneer een kleinschalige A1 bij schaalvergroting niet naar rechts maar naar boven verschuift, blijft er bij problemen voor ieder individu nog steeds niets tot nauwelijks iets aan de hand.

Het belang van PIA's

Voor een echt gefundeerde objectieve beoordeling heb je een privacy impact assessment (PIA) nodig. Het is jammer dat de AVG in artikel 35 de indruk wekt dat PIA's alleen in speciale gevallen verplicht zijn, maar lees dat artikel vooral als een extra harde aanbeveling bij het opzetten van nieuwe gegevensverwerkingen. Redenerend vanuit 39.2 en artikel 24-25 zijn PIA's, groot of klein, in wezen *altijd* nodig. Want een PIA is niet alleen een beoordelingstoets maar is ook de logische methodiek om tot passende maatregelen te komen.

Zie een PIA als een proces in vier stappen. Ze worden ook opgesomd in 35.7 AVG:

1. Zorg voor een goed beeld van de bestaande of beoogde gegevensverwerking. Over het algemeen vergt dat inzicht in de werkprocessen, onderliggende informatiestromen, en vormen van gegevensuitwisseling met zowel interne als externe partijen. Verlies je niet in details, maar hou het coherent en overzichtelijk. Kortom je wilt een systematische beschrijving van het geheel (de informatieketen in beeld).

2. Vervolgens wil je inzicht hebben in de categorieën gegevens die in iedere stap van het werkproces nodig zijn, om te kunnen beoordelen of de informatievoorzieningen toereikend

zijn: wie moet op welk moment (kunnen) beschikken over welke informatie? Dit is het onderzoek naar de noodzaak en evenredigheid.

3. Stap 3 is het ontwikkelen van realistische scenario's waardoor verstoring van het proces plaatsvindt.[5] Je gaat daarvoor beginselen van artikel 5 af. Bijvoorbeeld: 'Welke praktijksituaties kennen we waarbij we te maken hadden met *on*toereikende informatievoorzieningen, *on*juiste informatie of *on*voldoende beveiligde gegevens? Of; in welke situaties kan ons dat overkomen? Of; hoe kunnen problemen bij anderen ons ook overkomen? [6] Wat waren/zijn de gevolgen voor onze doelgroepen en onze organisatie? En hoever sloeg/slaat de meter dan uit op de Schaal van Erg?'

4. Tenslotte is het zaak om uit de praktijkscenario's het meest optimale pakket aan organisatorische en technische maatregelen te destilleren. 'Optimaal' wil zeggen dat ze logischerwijs tegengaan dat de probleemscenario's zich nog kunnen voordoen, ook rekening houdend met de stand van de techniek en de uitvoeringskosten, zoals 25 AVG benadrukt. Ook hier geldt; verlies je niet in de details maar bewerkstellig een handzaam overzicht van praktische kerneisen, die vooral ook doenlijk moeten zijn.

Besluit

De wetgever zegt nogal wat met dat ene zinnetje in 39.2. Want wat maakt een goede FG? Nou – dat je risicogestuurd opereert. En dat betekent dat je een werkwijze hanteert zoals hiervoor beschreven. Als je dat goed doet, vallen woorden als risico, aard, omvang context, verwerkingsdoeleinden en rechten en vrijheden, vanzelf op hun plek. We zagen ook dat je hiermee de verbinding legt tussen je eigen opdracht en de opdracht van verwerkingsverantwoordelijken in artikel 25-26 AVG. Want er moet worden voorzien in passende maatregelen. Maar zonder behoorlijk risicobegrip snapt niemand wat er gebeuren moet.

Het maakt niet zoveel uit of je FG bent voor een verwerkingsverantwoordelijke of een verwerker, want je werkt allebei toe naar juiste oplossingen. Verwerkers moeten zich kunnen inleven in de behoefte van de klant. Juist dan helpt het praten volgens de Schaal van Erg. Want als de klant C2-oplossingen nodig heeft, terwijl de verwerker excelleert in B2-oplossingen, is dat service level-niveau niet afdoende (niet passend).[7]

Help zowel jouw organisatie als de klant om dit te begrijpen. Denk desnoods mee over alternatieven, maar laat het niet zover komen dat C2-data de B2-omgeving binnenstroomt. Want dat is vragen om ongelukken – *ernstige* ongelukken bij C2's. Zo'n ongeluk kan op de verwerker vervolgens weer terugslaan in de vorm van ernstige reputatieschade, waardoor klanten vertrekken (C2 voor de verantwoordelijke blijkt voor de verwerker een C3).

Voorzien in passende maatregelen volgens artikelen 24 en 25 wil niet zeggen dat zich geen incidenten meer kunnen voordoen of dat er geen discussie meer kan ontstaan. Oplossingen voor risicobeheersing worden in de praktijk voortdurend ge*challenged*, maar dat is prima. Zie erop toe dat PIA's na verloop van tijd worden herijkt, leer van incidenten en zorg ervoor dat oplossingen worden bijgesteld waar dat nodig blijkt, want passendheid van maatregelen vergt permanent aandacht.

Voor nu is het belangrijk dat oplossingen eerst in de praktijk worden gebracht. Ook dat bewaak je als FG. Maar daarover meer in deel 3 van deze reeks 'Wat maakt een goede FG?'.

---

[5] Ook de EDPB geeft aan dat in scenario's moet worden gedacht. Zie de Guidelines on Data Protection Impact Assessment (wp248rev.01), p.6.
[6] Diverse instanties zoals de Nationale Ombudsman en de Algemene Rekenkamer hebben rapporten gepubliceerd waar veel uit te leren valt.
[7] Artikel 28.1 AVG.

Colofon

Privacy Management Partners is een FG-bureau. De wet passen wij toe in onafhankelijkheid en conform de bedoeling. Onze partners volgen sinds 1988 het wetgevingsproces en zijn daar sinds 1998 actief bij betrokken. Maar bovenal zijn wij geworteld in de praktijk. Dat levert andere resultaten op en een ander geluid dan u misschien gewend bent.

Privacy Management Partners

Vondellaan 46
3521 GH Utrecht
T 085-401 3866
W www.pmpartners.nl
E info@pmpartners.nl