TECHNISCHE NOTA

Uitschrijven en implementeren van GDPR Procedures

Een van de essentiële begrippen bij de implementatie van de GDPR-verordering is het woord ”accountability” wat betekent dat de entiteiten die binnen het toepassingsveld van deze regelgeving vallen verantwoording moeten kunnen afleggen, indien ze hierover worden geïnterpelleerd.

Het is dus van belang dat het kantoor kan bewijzen dat ze de bepalingen van deze verordening effectief naleeft.

Enig formalisme is dus vereist, maar het ligt voor de hand dat de graad van formalisering en documentering afhangt van de taille van het kantoor.

Het is alleszins van belang dat het kantoor procedures uitschrijft, deze implementeert en kan bewijzen dat ze deze uitgeschreven regels toepast.

Accountability betekent dat een kantoor kan verantwoorden dat ze de opgelegde principes en regels kan respecteren. De principes zijn vastgelegd in de verordening, maar de concrete regels kan een kantoor zelf uitwerken. Dit moet dan wel geschieden op basis van het risicoprofiel van de organisatie dat moet ingeschaald worden in functie van de specifieke vereisten van de bescherming van de persoonsgegevens.

Die interne regels hoeven niet dermate restrictief te zijn dat er zich geen incidenten kunnen voordoen, maar de organisatie moet er wel zorg voor dragen dat het risico op incidenten beperkt blijft en dat in voorkomend geval gepaste maatregelen worden genomen.

We overlopen hierna enkele mogelijke pistes, thema’s, overwegingen en bekommernissen die kunnen helpen bij het uitschrijven van deze procedures.

Kantoren die een kader van interne kwaliteitsbeheersing hebben opgezet, het weze omdat zulks verplicht is, het weze omdat ze zulks op vrijwillige basis doen, dienen deze GDPR-procedures vanzelfsprekend te integreren in het geheel.

Omdat de bewaking van persoonsgegevens geen losstaand gegeven is, volstaat het niet één specifieke GDPR procedure uit te schrijven, maar dienen ook alle andere procedures die rechtstreeks of onrechtstreeks te maken hebben met de inwinning en bewaring van persoonsgegevens tegen het licht gehouden te worden.

Persoonsgegevens impact beoordeling (de preliminaire risico-inschatting)

Bij het opzetten van de procedures hoort elk kantoor minstens een evaluatie te maken van de belangrijkste risico's waaraan het onderhevig is, en van de impact van eventuele inbreuken.

In de verordening heeft men het over de Data Protection Impact Assessment (DPIA) welke in een aantal gevallen zelfs verplicht is. We mogen ervan uitgaan dat dit niet het geval is voor de meeste economische beroepsbeoefenaars.

Aan de hand van zulke preliminaire analyse kan men oordelen of en welke procedures horen te worden uitgewerkt voor elkeen van de mogelijke risicogebieden.

Voorbeelden:

- Economische beroepsbeoefenaars die vaak te maken hebben met fysische personen (zoals bijvoorbeeld bij de indiening van de aangifte tot de personenbelasting) zullen een groter risico lopen dan deze die zich enkel met rechtspersonen bezig houden ;
- Economische beroepsbeoefenaars die werken voor "privacy-gevoelige" sectoren (medische sector, strafrechterlijke expertisen, religieuze gemeenschappen, ...) zullen hun risico hoger moeten inschalen;
- Economische beroepsbeoefenaars die bij hun werkzaamheden "big data" hanteren lopen een hoger risico dan deze dit met specifieke en beperkte data werken;
- Wanneer de beveiligingsmaatregelen op het vlak van intrusie, diefstal, verduistering, vervalsing gering zijn, zal het risico op incidenten hoger liggen;
- Gegevens met betrekking tot minderjarigen worden in de verordening met bijzonder aandacht beschouwd wat op zich dus ook leidt tot een andere risico-inschatting;
- Indien de activiteit de uitwisseling van persoonsgegevens met andere landen inhoudt die er geen strikt beleid inzake de privacy op na houden dient dit risico hoger ingeschaald te worden;
- Indien de persoonsgegevens voor meerdere doeleinden worden ingezameld houdt dit mogelijk een hoger risico in (herbestemming van persoonlijke gegevens);
- Indien persoonsgegevens worden ingewonnen op een consensuele basis eerder dan op een wettelijke of een contractuele basis, impliceert dit een hoger risico;
- Economische beroepsbeoefenaars die werken met veel verwerkers lopen meer risico dan deze die daarvan minder gebruik maken;
- Indien de beroepsbeoefenaar reeds beschikt over een formeel kader van deugdelijk uitgewerkte en toegepaste interne kwaliteitstoetsing dan draagt dit kantoor vermoedelijk een lager risico.

Procedure inzake het opzetten en het de periodieke bijwerking van het dataverwerkingsregister

Het heeft niet veel zin een procedure uit te schrijven voor de ontwikkeling van het dataverwerkingsregister. Het gaat immers om een eenmalig gegeven. Maar het is wel van belang te verifiëren dat dit register volledig is en de gegevens bevat die het hoort te bevatten.

Het is daarentegen wel aangewezen om concrete afspraken te maken omtrent de periodieke update van dit dataverwerking register.

Immers, doorheen de tijd is het best mogelijk dat de aard, het voorwerp, het doel van de bewaarde persoonsgegevens wijzigen, net zoals het best mogelijk is dat men gebruik maakt van nieuwe communicatietechnieken en -middelen bij de gegevensverwerking.

Zulke periodieke bijwerking wordt best geformaliseerd en gedocumenteerd aan de hand van een specifieke procedure waarbij minstens hoort te worden uitgeschreven:

- Wie instaat voor deze periodieke review (a priori, de ad hoc aangestelde persoon)
- Met welke frequentie dit geschiedt: bij voorbeeld jaarlijks tenzij er structurele wijzigingen zijn die een snellere aanpassing van het register vereisen;
- Op welke wijze dit geschiedt
- Op welke wijze dit wordt gecommuniceerd en aan wie?

Bij een periodieke update van het register is het tevens nuttig om een “versioning” (referenceren en archiveren van opeenvolgende versies) bij te houden teneinde op te volgen welke versie precies tijdens welke periode gold.

Procedure inzake de toegankelijkheid, de beveiliging en de bewaring van data

Het spreekt voor zich dat deze procedure een wezenlijk deel is van het voorkomingsbeleid en dus de nodige aandacht verdient.

Kantoren met een intern kwaliteitsbeheersingssysteem hebben, a priori, reeds een procedure uitgewerkt waarin de beveiliging en de bewaring van data is geregeld zoals is geregeld in punt 46 van ISQC1 : “*Le cabinet doit définir des politiques et des procédures destinées à assurer la confidentialité, l'archivage sécurisé, l'intégrité, l'accessibilité et la facilité de recherche de la documentation d’une mission”* met toelichting in de paragrafen. A56 – A59 van ISQC-1

De bewaring van documenten wordt geregeld in paragraaf 47: “*Le cabinet doit définir des politiques et des procédures pour la conservation de la documentation des missions pendant une période de temps suffisante pour répondre à ses besoins ou aux exigences de la loi ou de la réglementation* met toelichting in de paragrafen. A60 – A63.

Het verdient dan ook aanbeveling om de in het kader van ISQC1 uitgewerkte, in zoverre als nodig, aan te vullen met specifieke passages welke de bewaring en beveiliging van persoonsgegevens

behandelen. De voorbeeldprocedures beschikbaar op de website van het ICCI kunnen daarbij van nut zijn.

Bij de bewaring van gegevens mag men niet uit het oog verliezen dat de persoonsgegevensbescherming niet enkel betrekking heeft op elektronische gegevens, maar ook fysische data.

Dit onderscheid wordt ook best doorgetrokken in het procedureboek wat betekent dat men zich, vooraf de vraag moet stellen:

- Op welke wijze de persoonsgegevens worden bewaard (hard copy, elektronisch, digitaal)
- Waar de fysische gegevens worden bewaard (fysisch in lokale bewaring of geëxternaliseerd zoals de archieven, op beveiligde manier, of eenvoudig toegankelijk)
- Waar de elektronische gegevens worden bewaard : PC, lokale computer, server, in de “cloud”.

  Merk op dat de gegevensverwerkingsverantwoordelijke de verantwoordelijke is en de cloud serviceprovider een onderaannemer (“verwerker”) is. Het komt aan de verantwoordelijke toe een onderaannemer te kiezen die de gepaste garantie biedt dat de verplichtingen van de GDPR-verordening worden nageleefd;

- Van welke digitale gegevensdragers er gebruik wordt gemaakt (USB, CD, DVD, ...)
- Wie toegang heeft tot deze gegevens,

Daarbij kunnen de volgende thema’s, risico’s en veiligheidsmaatregelen worden aangekaart:

- Beperkingen tot toegang tot het informaticaplatform (authentificatietechnieken en methode, paswoorden, vingerafdrukdetectie, ...)
- Encryptie van de gestockeerde data (in het bijzonder bij draagbare PC);
- Toegangsrestricties tot enkel deze gegevens welke noodzakelijk zijn voor de werkzaamheden;
- Verplichte periodieke wijziging van het paswoord;
- Fysische beveiliging van de computers met inbegrip van een politiek inzake bewaring van computers bij verplaatsingen, thuiswerk, gebruik op verplaatsingen
- Intrusie en hackingtesten uitbesteed aan derde deskundigen
- Service level agreement met externe leveranciers, dienstverstrekkers en andere partijen waarin een expliciete voorzieningen inzake het gebruik en de bewaring van persoonsgegevens worden opgenomen
- Voor de gegevens bewaard door middel van cloud computing, verificatie of de gegevensverwerker (de *cloud service provider)* de GDPR-verordening en de Europese Richtlijn over Netwerk- en Informatieveiligheid (NIS-richtlijn) van 6 juli 2016 naleeft – Hier beschikbaar;

Indien de voorbeeldteksten van het ICCI niet zouden volstaan of niet volledig van toepassing kunnen zijn, kunnen ook een aantal veiligheidsvoorschriften afgeleid uit de verzekeringspolissen, welke specifieke risico’s inzake informatieveiligheid, computercrime, hacking, en dergelijke meer dekken.

Aanstelling en taken van een ad hoc verantwoordelijke inzake bewaking van persoonsgegevens

De verordening voorziet expliciet[1] in een aantal gevallen de verplichting tot het aanstellen van een zogenaamde *data protection officer* (in het Nederlands: "*de functionaris voor de gegevensbescherming"*[2]). De drempels zijn vooral activiteit gebonden[3] wat betekent dat een de beroepsbeoefenaars in de economische sector, a priori, niet aan deze verplichting zullen onderworpen zijn.

We onthouden vooral dat er geen mathematisch criterium wordt gehanteerd bij de toetsing of er een DPO wordt aangesteld of niet, maar dat men zich vooral de vraag moet stellen of de uitgeoefende activiteit een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen.

In beginsel is dit niet het geval voor de economische beroepsbeoefenaars.[4]

Deze beroepsbeoefenaars kunnen mogelijk wel onrechtstreeks uitgenodigd worden om een DPO aan te stellen. Dit kan het geval zijn wanneer een beroepsbeoefenaar bijvoorbeeld optreedt als "verwerker" voor een andere entiteit zoals een overheidsinstantie of –overheidsorgaan, welke gehouden is een DPO aan te stellen.

Dit neemt niet weg dat kantoren op vrijwillige basis wel een *ad hoc* verantwoordelijke kunnen aanstellen. De drie instituten bevelen overigens aan dat zulks ook effectief gebeurt, zelfs binnen de kantoren van een eerder kleinere taille.

Deze functie kan ook worden uitbesteed aan een derde. In dat geval komt het eropaan dat deze externe deskundige over de gepaste competentie en tijd beschikt, maar ook op een snelle en toegankelijke wijze kan communiceren met het kantoor.

Bij de aanstelling van een ad hoc verantwoordelijke mag men niet uit het oog verliezen dat de functie van *data protection officer* expliciet is geregeld in de verordening, wat betekent dat het wettelijk dispositief zoals uitgeschreven in deze regelgeving ook van toepassing is op de persoon die wordt aangesteld als *data protection officer*.

Dit is mogelijk niet altijd wenselijk[5]. In zulke gevallen kan het kantoor overwegen om een andere titel te geven aan deze functie (zoals bijvoorbeeld privacy officer, GDPR-officer, ...) zodat er geen misverstand kan bestand rond de vraag of de GDPR-plichten (en rechten) die krachtens de verordening wegen op een DPO ook van toepassing zijn op de aangestelde ad hoc persoon.

---

1 Hoofdstuk IV, afdeling 4, artikelen 37 tot 39;

2 Onder de Richtlijn 95/46/EG reeds gekend onder de naam "functionaris voor de gegevensbescherming*";*

3 In de oude richtlijn onthouden we onder meer de drempel van 250 werknemers als referentie. De vrijstelling voor KMO's is weggevallen in de nieuwe verordening.
In de verordening onthouden we vooral dat deze verplichting geldt wanneer er sprake is van een verwerking welke regelmatige en stelselmatige observatie op grote schaal als kerntaak inhoudt, ofwel de grootschalige verwerking van bijzondere categorieën als kerntaak.

4 Het niet aanstellen van een DPO wanneer dit wel nodig is kan leiden tot een administratieve sanctie.

5 De DPO geniet bijvoorbeeld van een ontslagbescherming

Indien effectief een DPO wordt aangesteld houdt in ook dat een aantal plichtplegingen worden nageleefd zoals:

- Vermelding van DPO in de informatie die de verantwoordelijke aan de betrokkene meedeelt (artikel 13);
- Mededeling van de contactgegevens van de DPO (artikel 14);
- Opname van contactgegevens DPO in het register van de verantwoordelijke en de verwerker (artikel 30);
- Mededeling van een inbreuk aan de toezichthoudende autoriteit (artikel 33) en aan de betrokkene (artikel 34);
- Tussenkomst van de DPO bij de gegevensbeschermingseffectbeoordeling (artikel 35)

Op welke wijze en met welke titel de functie ook wordt ingevuld, het lijkt evident dat de aangestelde betrokkene, zijn taak ter harte neemt, en deze alleszins uitvoert naar de geest van de verordening. Indien hij als DPO wordt aangesteld is dit echter ook een reglementaire verplichting. Zijn taken behelzen de informatieverstrekking (wat een kennis van het wettelijk kader veronderstelt), de adviesverstrekking (bijvoorbeeld bij de impact assessment) en toezicht uit te oefenen op de naleving van de verordening. Wat dit laatste punt betreft is hij in zekere zin dus ook voor een stuk begaan met *"compliance".*

De aangestelde verantwoordelijke heeft ongetwijfeld ook een sensibiliseringsrol en een opleidingstaak: hij dient zijn werkomgeving bewust te maken en alert te houden voor alle aangelegenheden die met persoonsgegevens te maken hebben.

In zoverre zulks opportuun lijkt brengt de ad hoc verantwoordelijke (periodiek) verslag uit aan het hoogste leidinggevende orgaan, zoals dit ook wordt verwacht van andere functies zoals de interne audit, de compliance, riskmanagement, enz.

Procedure inzake de rapportering van incidenten

Ingeval een incident zich voordoet dient de gegevensverwerkingsverantwoordelijke, in principe, binnen een periode van 72 uur nadat hij op de hoogte werd gebracht zulks mee te delen aan het toezichthoudend orgaan[6], en in sommige gevallen ook aan de betrokkene.

De regels zijn soepeler voor de verwerkers[7] wat rechtsonzekerheid kan creëren. Het verdient daarom aanbeveling in de contracten tussen gegevensverwerkingsverantwoordelijke en de gegevensverwerker ook een termijn af te spreken omtrent mogelijke incidentrapportering.

De procedure inzake incidentrapportering kan eenvoudig en beknopt worden gehouden, en zou bijvoorbeeld kunnen bevatten:

- Vorming en bewustwording van de medewerkers inzake incidenten en de toe te passen procedure;

[6] Artikel 33, eerste paragraaf;
[7] Artikel 33, tweede paragraaf;

- Politiek inzake het beheer van verwerkers met een contractuele regeling o.a. in verband met de meldingsplicht;
- Uitgeschreven richtlijnen voor de medewerkers die met een incident wordt geconfronteerd
- Uitgeschreven richtlijnen voor de ad hoc verantwoordelijke die met een incident wordt geconfronteerd, met inbegrip van de verplichte mededeling aan de toezichthoudende autoriteit en aan de betrokkenen
- Principes, regels en richtlijnen inzake de melding en de bijstand bij inbreuken in verband met persoonsgegevens
- Draaiboek en mogelijke scenarii om de nadelige gevolgen van het incident tot een minimum te beperken;
- Nuttige adressen en contacten van personen die bijstand kunnen verlenen
- Template van een incidentrapportering

Procedure inzake aanwerving en opleiding personeel

De sensibilisering van personeel op het vlak van de bescherming van persoonsgegevens is ongetwijfeld van belang, maar behoeft daarom geen periodieke vorming of specifieke opleiding, en dus ook geen specifieke procedure.

Het is daarentegen wel van belang dat het thema wordt aangekaart bij de rekrutering van personeel, maar ook van tijdelijke krachten.

Meest aangewezen lijkt in dit verband om deze sensibilisering en een korte voorstelling van het wettelijk kader in te lassen in de procedure welke geldt bij de aanwerving van nieuw personeel, waarbij ook de andere kantoorprocedures worden voorgesteld en besproken (“intake”-gesprek).

Sectoriële gedragscode

Het artikel 40 van de Verordening spoort onder meer de lidstaten en de toezichthoudende autoriteiten aan om gedragscodes te laten ontwikkelen welke rekening houden met de specifieke kenmerken van de diverse gegevensverwerkingssectoren en de specifieke behoeften van kleine, middelgrote en micro-ondernemingen.

De drie instituten hebben het voornemen om gezamenlijk zulke *code of conduct* op te stellen waarbij nog moet worden uitgemaakt op welke wijze deze code kan worden geïntegreerd in het normatief kader.

Deze zal, zoals voorgeschreven door de Verordening, ter goedkeuring worden voorgelegd aan de Gegevensbeschermingsautoriteit.

Certificatie

De interne kwaliteitsbeheersing kan soms ook worden opgelegd door tegenpartijen zoals klanten of leveranciers die enkel wensen te werken met deugdelijke ondernemingen, welke de regels inzake de bescherming van persoonsgegevens respecteren.

Het valt dus niet uit te sluiten dat tegenpartijen niet meer wensen te werken met de beroepsbeoefenaar, indien die niet het bewijs kan voorleggen dat hij een gepast beleid en beheerssysteem heeft.

De bedrijfsrevisoren kunnen in zulk geval verwijzen naar de norm ISQC-1. Andere beroepsbeoefenaars kunnen deze norm op vrijwillige basis toepassen.

Een mogelijk alternatief waarmee tegenpartijen vrede kunnen nemen is de verkrijging van een extern certificaat (vb. ISO 27001).

Nog enkele tips & tricks

Indien het kantoor of een aantal van haar leden een relatief atypische activiteit uitoefenen of een atypisch cliënteel hebben is het raadzaam de verordening in detail te lezen.

In de regelgeving zijn immers een aantal striktere regels opgenomen, om specifieke (groepen van) personen een bijkomende bescherming te bieden.

Het is in dat geval van belang om weten dat deze strengere regels wel of niet van toepassing zijn.