BEYOND THE GDPR

Nu 25 mei 2018 steeds dichterbij komt, ligt er een sterke focus op de implementatie van de General Data Protection Regulation (GDPR). Dat lijkt een logische actie, maar is het wel voldoende? Volgens Arie Linsen moeten we breder kijken en direct informatiebeveiliging of direct ontwikkelingen meenemen.

door Arie Linsen

IN DE GENERAL DATA PROTECTION REGULATION (GDPR) WORDT OP VERSCHILLENDE PLAATSEN verwezen naar het beveiligen van de verwerking van persoonsgegevens. Zo staat in artikel 32 'Beveiligen van de verwerking' dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen moeten treffen om het risico, afgestemd op het beveiligingsniveau, te waarborgen. Onder het woord 'passend' wordt dan onder andere aangegeven:

- Pseudonimisering en versleuteling van persoonsgegevens.
- Het garanderen van de betrouwbaarheid, vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkingssystemen en diensten.
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.
- Een procedure regelmatig testen, beoordelen en evalueren.

Zo staat in artikel 25, 'Gegevensverwerking door ontwerp en door standaardinstellingen', dat gedurende het ontwikkeltraject rekening moet worden gehouden met de belangen van betrokkenen. De privacy moet worden gewaarborgd.
In het verlengde daarvan dienen de maatregelen als default in praktijk te worden gebracht.

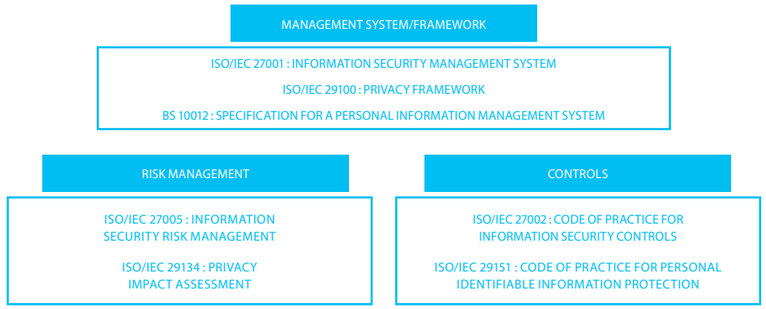
CERTIFICERINGSMECHANISME

In verschillende artikelen is aangegeven dat een certificeringsmechanisme kan worden gebruikt om aan te tonen dat passende technische en organisatorische maatregelen zijn genomen en dat de design- en default-principes worden toegepast. Daarvoor kan de certificering van de ISO 27001/2 als uitgangspunt worden genomen. Op zich een logische gedachtegang. Daarmee wordt een bepaalde garantie afgegeven dat de informatiebeveiliging volgens een bepaalde structuur is ingericht en dat dit ook op de agenda van het management staat. Het is geen 100% garantie, maar het geeft toch enige vorm van zekerheid. Zeker als je bedenkt dat veel maatregelen die moeten worden genomen, beveiligingsmaatregelen zijn.

Toch is die certificering niet zomaar een-op-een over te nemen. Er is niet voor niets een nieuwe ISO-standaardisatielijn in ontwikkeling. Zo wordt in de ISO 29100-standaard een raamwerk beschreven voor de bescherming van persoonsgegevens binnen de informatie- en communicatietechnologiesystemen. Het raamwerk is van algemene aard en plaatst organisatorische, technische en procedurele aspecten in een algemeen privacykader. Denk daarbij aan:

- algemene privacyterminologie;
- definities van actoren en rollen bij de verwerking van persoonsgegevens;
- beschrijving van de privacybeschermingsoverwegingen;
- beschrijving van de elf privacyprincipes.

Dit raamwerk kan gezien worden als een basis om invulling te geven aan andere normenkaders die betrekking hebben op persoonsgegevens.



De British Standards Institution (BSI) heeft een standaard (BS: British Standard) gepubliceerd over de specificatie van een Personal Information Management System. Dat is de privacytegenhanger van het Information Security Management System ISO 27001. Het zijn twee managementsystemen, maar wel beschreven vanuit een ander perspectief. In de British Standard komen de gangbare privacyaspecten aan bod die terug te vinden zijn in de GDPR.
De twee managementsystemen vormen in combinatie met het privacyraamwerk het managementsysteem om invulling te geven aan het privacyvraagstuk dat voortvloeit uit de implementatie van de GDPR.
Voor risicomanagement bestaan er ook weer twee invalshoeken om de verschillende risico's het hoofd te bieden. Zo wordt binnen de informatiebeveiliging teruggegrepen naar de ISO 27005, 'Information security risk management', en voor de privacy is er ISO 29134, 'Privacy impact assessment'. Ook hier geldt weer dat vanuit de verschillende invalshoeken risico's moeten worden gemitigeerd naar een aanvaardbaar niveau.

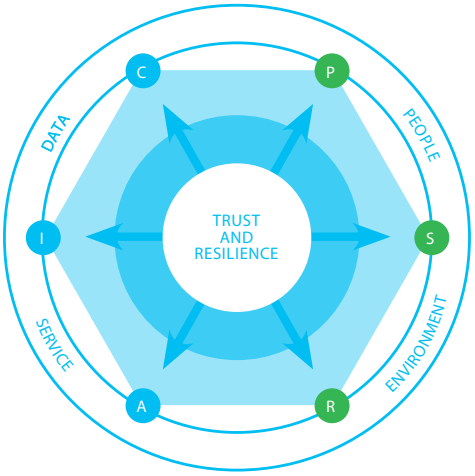
Uiteindelijk gaat het erom dat de juiste maatregelen worden gekozen om de bedrijfsvoering te kunnen waarborgen c.q. garanderen, zowel vanuit informatiebeveiligingsperspectief als privacyperspectief. De ISO 27002 is voor informatiebeveiliging al jaren een standaarddocument om invulling te geven aan de beveiliging van de informatievoorziening. Voor privacy is daar onlangs de ISO 29151 aan toe gevoegd. De ISO 29151 'Code of practice for personally identifiable information protection' heeft dezelfde structuur als de 27002 voor informatiebeveiliging. In dit document wordt aangegeven of de maatregelen van toepassing zijn voor de privacy.
Daarnaast wordt in een aantal gevallen een "Implementatie leidraad voor de bescherming van persoonsgegevens" toegevoegd. Tevens is een Annex A toegevoegd, met een set van aanvullende maatregelen voor de beveiliging van persoonsgegevens. Dat zijn de uitgewerkte privacyprincipes uit de ISO 29100.

CLOUDCOMPUTING

Nu cloudcomputing een vast onderdeel is geworden van ons dagelijkse leven en steeds meer verwerkingen in de cloud worden afgewerkt, dient goed te worden nagedacht over de beveiligingsmaatregelen. In eerste instantie wordt dan vaak teruggegrepen op de maatregelen uit de Code voor Informatiebeveiliging.
Een goede basis, maar die dient wel te worden aangevuld met de aanvullende maatregelen die in de ISO 27017 specifiek gelden voor cloudservices.
In dat normenkader staan ook nog aanvullende richtlijnen voor cloudgebruikers en cloudserviceproviders.
In cloudomgevingen worden veel persoonsgegevens verwerkt en dan is de GDPR weer van toepassing. Ook voor de cloudomgeving is een standaard ontwikkeld, ISO 27018, die op identieke manier is ingestoken als de ISO 29151. Uitgangspunt zijn de maatregelen uit de 27002, aangevuld met privacymaatregelen en de elf eerdergenoemde privacyprincipes. Tevens zijn er weer implementatierichtlijnen genoemd bij de verschillende onderdelen, zowel voor de gebruiker als de cloudserviceprovider.

ONDOORZICHTIGER

Al met al lijkt het door al die ISO-standaarden alleen maar ondoorzichtiger te worden. Op zich valt het wel mee.
We hebben de beveiligingsmaatregelen, die worden aangevuld met privacymaatregelen als er sprake is van verwerking van persoonsgegevens. Dit klinkt erg simplistisch, maar daarbij dienen wel de juiste afwegingen te worden gemaakt.
De cloud speelt een voorname rol in de digitale transformatie waarin wij ons bevinden. Die digitalisering heeft ook grote gevolgen voor het speelveld van informatiebeveiliging en privacy.
De veranderingen zijn al zichtbaar, maar de grote veranderingen komen nog. Gartner heef de afgelopen jaren al verschillende veranderingen besproken. Confidentiality, Integrity en Availability (CIA) zijn niet langer voldoende om de beveiliging op het gewenste niveau te krijgen en te houden. Deze beveiligingseisen richten zich primair op de data en de services.
Doordat de digitale wereld steeds meer samensmelt met de reële wereld, komt de mens steeds in het centrum te staan. Gartner positioneert daarom Privacy, Safety en Reliability (PSR) in het spectrum van de beveiliging, waarbij die laatste drie aspecten zich richten op de mens en zijn omgeving. De CIAPSR vormen de basis in de cybersecurityscope. De Privacy in het model wordt door Gartner direct gerelateerd aan de European Union GDPR. Daarmee wordt aangegeven dat de werkingssfeer van de GDPR wereldwijd gevoeld wordt en dat daar expliciete aandacht aan moet worden gegeven. De Privacy is in dit model ook een onderdeel van het totaalconcept voor beveiliging.
Een integrale benadering past ook beter, omdat privacy en informatiebeveiliging niet los van elkaar gezien kunnen worden. Daarbij kunnen de verschillende ISO-standaarden, inclusief de BS-standaard, zeker een belangrijk hulpmiddel zijn. Zij geven in elk geval de kaders aan waarbinnen informatiebeveiliging en privacy kunnen worden vormgegeven. Daarbij zullen de risicomanagementmethodieken zeker van pas komen om de juiste mitigerende maatregelen te nemen om organisaties veilig en betrouwbaar te laten functioneren.



AUTEUR

ARIE LINSEN
Arie Linsen is zelfstandig consultant, gespecialiseerd in informatiebeveiliging, privacy en informatiemanagement, en tevens docent bij de Security Academy op de genoemde gebieden.