Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens[1]

Versie 1.0

Het voorliggend document bevat een lijst met elf actiedomeinen in verband met de informatiebeveiliging waarvoor elke instelling – rechtspersoon[2], onderneming of administratie – die persoonsgegevens bewaart, gebruikt, verwerkt of mededeelt, maatregelen moet nemen.

De extreme diversiteit van concrete situaties maakt het onmogelijk om voor elk voorkomend geval heel precies de te ondernemen acties te omschrijven.

Elke hiernavolgende referentiemaatregel zal dus aan de context en aan het specifieke karakter van elke instelling aangepast moeten worden en impliceert de uitvoering van praktische oplossingen waarvan het detailniveau of de complexiteit proportioneel moet zijn ten opzichte van de reële behoeften van de instelling. Hiervoor moet rekening worden gehouden met:

- de aard van de verwerkte persoonsgegevens en de verwerkingen ervan evenals de vereisten inzake vertrouwelijkheid, integriteit en beschikbaarheid;
- de wettelijke of reglementaire vereisten die van toepassing zouden zijn;
- de grootte van de instelling (daarbij inbegrepen het aantal personen die toegang tot de gegevens zouden kunnen hebben);
- het belang en de complexiteit van de betrokken informatiesystemen, toepassingsprogramma's en informaticasystemen;
- de mate waarin de instelling openstaat voor de buitenwereld evenals de mate waarin er toegang is vanuit de buitenwereld;
- de risico's waaraan de instelling zelf of de personen wiens persoonsgegevens worden verwerkt zich blootstellen;
- alsook de 'stand van de techniek terzake en de kosten voor het toepassen van de maatregelen'[3].

Informatiebeveiliging is een materie die blijvend onderhevig is aan evolutie en daarom zullen deze referentiemaatregelen ook systematisch worden aangepast in functie van de ontwikkelingen van de regelgeving, de techniek of andere aspecten.

---

[1] Het voorliggend document is bestemd voor de verantwoordelijken van een verwerking en wil als hulp dienen bij de implementatie van een degelijke beveiliging overeenkomstig de verplichting opgelegd in artikel 16 van de Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van 8 december 1992.

[2] Dit stelt natuurlijke personen niet vrij van de verplichting zich te voegen naar artikel 16 van de Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, dat aan elke verantwoordelijke voor de verwerking verplichtingen oplegt inzake beveiliging.

[3] Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van 8 december 1992.

1. Informatiebeveiligingsbeleid

Elke instelling die persoonsgegevens gebruikt/verwerkt moet een geschreven document opstellen – het informatiebeveiligingsbeleid – waarin de strategieën en de weerhouden maatregelen voor gegevensbeveiliging nauwkeurig worden omschreven.

Vooraleer deze beveiligingsstrategieën en -maatregelen bepaald worden, moet de instelling nadenken over de potentiële dreigingen die wegen op de gebruikte/verwerkte persoonsgegevens en de reële risico's waaraan deze gegevens blootstaan evalueren.

Het informatiebeveiligingsbeleid bestaat uit:

- een toelichting over de uitgevoerde analyse en het risicobeheer van de persoonsgegevens;
- de prioriteiten die werden weerhouden en de beheersmaatregelen die ingevolge deze risicoanalyse werden of worden aangebracht;
- de planning van de inwerkingstelling;
- de beschrijving van de verschillende verantwoordelijkheden en de ingestelde organisatorische regels;
- de beschrijving van het beheersproces bij beveiligingsincidenten;
- de beschrijving van het sensibiliseringsproces van de instelling voor dit beleid;
- de weerhouden maatregelen om het beveiligingssysteem te actualiseren eens het werd geïnstalleerd.

Dit informatiebeveiligingsbeleid moet door de hoogste hiërarchie en de diverse verantwoordelijken worden goedgekeurd en opdat dit beleid bij iedereen gekend zou zijn, moet het binnen de instelling voldoende verspreid worden.

Dit beleid moet ten minste een keer per jaar of na wijziging of herevaluatie worden bijgewerkt.

2. Organisatie van informatiebeveiliging

Al naargelang van de aard van de gebruikte/verwerkte persoonsgegevens en de termen van de verleende machtiging moet binnen de instelling een veiligheidsconsulent worden aangesteld die verantwoordelijk is voor de uitvoering van het informatiebeveiligingsbeleid.

De veiligheidsconsulent rapporteert rechtstreeks aan de directie van de instelling, en moet kunnen beschikken over voldoende middelen (tijd, human resources, uitrusting en budget) en vrijuit toegang hebben tot de informatie die noodzakelijk is voor zijn functie en voor zover hij binnen het kader van het informatiebeveiligingsbeleid blijft.

Hij zal erop toezien dat de verschillende verantwoordelijkheden inzake informatiebeveiliging (preventie, toezicht, opsporing en verwerking) duidelijk in kaart zijn gebracht en dat de personen belast met de informatiebeveiliging in alle onafhankelijkheid kunnen handelen en ervan gevrijwaard blijven dat ze voor persoonlijke of tegenstrijdige belangen onder druk worden gezet.

De veiligheidsconsulent zal moeten beschikken over de noodzakelijke competenties en opleidingen en zal geen functie(s) kunnen uitoefenen of verantwoordelijkheden hebben die onverenigbaar zijn met die van veiligheidsconsulent.

3. Organisatie en menselijke aspecten van de informatiebeveiliging

De instelling moet duidelijk de verantwoordelijkheden en het beheersproces inzake beveiliging van persoonsgegevens omschrijven en die op gepaste wijze integreren in de algemene organisatiestructuur en werking.

Om de informatiebeveiliging te organiseren, moeten er voldoende en aangepaste organisatorische, technische en financiële middelen beschikbaar worden gesteld.

Om de persoonsgegevens op een doeltreffende wijze te beveiligen moet de instelling erop toezien dat er procedures worden opgesteld voor classificatie[4] van informatie. Dit maakt de inventarisatie en lokalisatie van alle gebruikte/verwerkte persoonsgegevens mogelijk, ongeacht het soort drager.

Omdat het welslagen van een beveiliging van een informatiesysteem sterk afhangt van een correcte informatieverstrekking aan de verschillende actoren, moet de instelling de nodige maatregelen nemen opdat elke persoon (intern of extern) die tussenkomt in de verwerking van persoonsgegevens, voldoende en constant geïnformeerd wordt over zijn verplichtingen en verantwoordelijkheden tijdens deze verwerking en voldoende en juist opgeleid is voor de uitoefening van zijn functies en verantwoordelijkheden inzake informatiebeveiliging.

Er moet eventueel in tuchtrechtelijke gevolgen worden voorzien ingeval de voorgeschreven regels niet worden nageleefd, en wanneer de risico's dit rechtvaardigen is een geheimhoudingsverklaring vereist.

Wanneer de instelling deze verwerkingen van persoonsgegevens geheel of gedeeltelijk in onderaanneming geeft, moet ze erop toezien dat in het contract van onderaanneming dezelfde verplichtingen inzake informatiebeveiliging opgenomen worden als die van de instelling zelf.

4. Fysieke beveiliging van de omgeving

De instelling moet de nodige maatregelen nemen om de fysieke bescherming van de persoonsgegevens te garanderen.

Hiertoe moet de instelling zich ervan verzekeren dat de dragers van persoonsgegevens en de informaticasystemen die deze gegevens gebruiken/verwerken overeenkomstig hun classificatie geplaatst worden in geïdentificeerde en beschermde lokalen waarvan de toegang beperkt is tot de hiertoe gemachtigde personen en tot de uren waarin zij hun functie uitoefenen.

[4] De term "classificatie" dient hier te begrepen volgens de klassieke bewoording van ordening van gegevens zoals het genoegzaam wordt aangewend bij beveiliging van informatiesystemen, d.w.z. kwalificatie van de informatie en niet zoals voorzien in de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

Wanneer een continuïteit van diensten noodzakelijk blijkt, moeten er apparaten geïnstalleerd worden ter preventie, opsporing en aanpak van fysieke bedreigingen zoals branden of overstromingen. Deze apparaten moeten regelmatig gecontroleerd worden. De instelling moet ook back-upmaatregelen nemen om het verlies of de toevallige verandering van de persoonsgegevens te verhinderen.

5. Beveiliging van de netwerken

De instelling moet zich ervan vergewissen dat de netwerken waarmee de apparatuur verbonden is en die betrokken is bij een gebruik/verwerking van persoonsgegevens, de vertrouwelijkheid en de integriteit van de gegevens garanderen.

Indien het interne netwerk van de instelling verbonden is met een openbaar extern netwerk dan moet de instelling de noodzakelijke maatregelen nemen om het (de) netwerk(en) tijdens de verwerkingen te beschermen tegen elke onrechtmatige toegang (inbraken, virussen, kwaadaardige software, enz.).

6. Logische beveiliging van de toegang

De instelling moet zich ervan vergewissen dat de persoonsgegevens overeenkomstig hun classificatie slechts toegankelijk zijn voor de personen en toepassingsprogramma's die hiertoe uitdrukkelijk gemachtigd zijn.

De instelling bewaart een bijgewerkte lijst van de verschillende personen die gemachtigd zijn om tot deze gegevens toegang te hebben en ze te gebruiken/verwerken, en van hun respectievelijke machtigingen.

Deze verschillende machtigingen moeten vertaald worden in technische voorzieningen en toegangscontroles tot de verschillende informaticaonderdelen (programma's, procedures, opslag, telecommunicatie-uitrusting) die tussenkomen in een verwerking van persoonsgegevens.

Deze technische voorzieningen moeten zowel vervat zitten in de activiteiten van de beginfase (ontwikkeling van de toepassingsprogramma's) als in die van de eindfase (back-upbeheer).

Indien het beveiligingsniveau het noodzakelijk maakt, zal de identificatie van de intervenanten vervolledigd worden met een authenticatie.

7. Logging, opsporing en analyse van toegang

De instelling moet loggings- en opsporingsmechanismen installeren.

Hiermee moet wanneer nodig de identiteit kunnen worden teruggevonden van iedere persoon die toegang had tot de persoonsgegevens of ze bewerkt heeft. De registratie van deze controle-informatie kan naargelang het geval betrekking hebben op fysieke toegang, logische toegang of beide.

De fijnheid van de registraties, de lokalisatie en de bewaarduur van deze gegevens, evenals de frequentie van de bewerking en het type bewerkingen, hangen af van de context. Bijkomende

mechanismen voor opsporing van inbraak zouden kunnen vereist zijn. De verantwoordelijke voor de verwerking moet in staat zijn de gemaakte keuzes te rechtvaardigen.

Omdat opsporingsgegevens persoonsgegevens zijn, moet elke verwerking van deze gegevens gepaard gaan met gepaste beheersmaatregelen.

8. Toezicht, nazicht en onderhoud

De instelling moet zich ervan vergewissen dat de technische of organisatorische beheersmaatregelen gevalideerd zijn en regelmatig nagekeken worden.

Om te bepalen hoe de informatiebeveiliging op een passend niveau kan worden gehouden, moet er toezicht worden gehouden op de verwerkingen, de evolutie van de bronnen en de analyse van de loggings.

Aangezien de informatiesystemen en de risico's waaraan zij blootstaan constant evolueren, dient de instelling er zich regelmatig van te vergewissen (minstens één keer per jaar) dat de aanvankelijk nagestreefde doelen en de maatregelen die daarna werden ingesteld nog actueel zijn, opdat ze indien nodig verbeteringen zouden kunnen aanbrengen.

Bij elke reorganisatie van de instelling of wijziging van haar infrastructuur moet er een actualisering van de beheersmaatregelen doorgevoerd worden.

9. Beheer van beveiligingsincidenten en continuïteit

De instelling moet beschikken over een beheersplan voor beveiligingsincidenten.

Wanneer er zich incidenten voordoen die de vertrouwelijkheid en de integriteit van de persoonsgegevens in gevaar brengen, is de snelheid van een interventie primordiaal om de gevolgen van een dergelijke situatie in de dijken. Hiertoe moet de instelling in procedures voorzien die nauwkeurig omschrijven welke de te ondernemen stappen zijn bij ontdekking van een beveiligingsincident van persoonsgegevens alsook welke personen verantwoordelijk zijn om dit incident aan te pakken en zo een gezonde toestand te herstellen.

Bovendien moeten de omstandigheden van het incident geanalyseerd worden, zodat er daaruit preventieve maatregelen of bijsturingen kunnen worden gefilterd om een herhaling van dit soort incidenten te vermijden of om zo snel mogelijk naar de normale toestand te kunnen terugkeren.

Instellingen die verplicht zijn om de continuïteit van hun diensten te verzekeren moeten:

- voorzien in een herstel- en continuïteitsplan om zich bij beveiligingsincidenten in te dekken tegen een dienstenonderbreking die de aanvaardbare termijn overschrijdt;
- er in het bijzonder op toezien dat tijdens de uitvoering van de diverse plannen de vertrouwelijkheid en de integriteit van de persoonsgegevens steeds gegarandeerd zijn.

10. Naleving

Elke instelling moet steeds alle van toepassing zijnde regels en wetten naleven met betrekking tot de verwerking en de bescherming van persoonsgegevens. Deze wetgeving is steeds raadpleegbaar op de website van de Privacycommissie in de rubriek "Wetgeving en normen".

Zo bepaalt de Privacywet heel nauwkeurig de voorwaarden en de omstandigheden voor een verwerking of doorgifte van persoonsgegevens. Elke instelling is verplicht om voorafgaand aan de verwerking na te gaan of de uitvoering van de verwerking, gelet op het delicate karakter van de gegevens, niet onderworpen is aan een machtiging en moet er steeds over waken dat de voorwaarden van de machtiging gerespecteerd blijven.

De instelling moet op regelmatige basis een audit organiseren met betrekking tot de beveiliging van de gebruikte/verwerkte persoonsgegevens.

11. Documentatie

De instelling moet beschikken over volledige, gecentraliseerde documentatie en die met betrekking tot informatiebeveiliging regelmatig bijwerken.

De instelling moet voor het goed beheer van beveiligde persoonsgegevens alle nodige documentatie aanleggen. Deze documentatie moet volledig en geformaliseerd zijn, proportioneel ten opzichte van de informatiebeveiligingsbehoeften, voortdurend worden bijgewerkt en geïnventariseerd zodat ze te gelegener tijd beschikbaar is voor de bevoegde persoon.

Deze documentatie moet ten minste het volgende bevatten:

- het informatiebeveiligingsbeleid;
- de identiteit van de veiligheidsconsulent of van de verantwoordelijke voor de informatiebeveiligingscel;
- de implementatie van de beheersmaatregelen;
- de inventaris van de gebruikte/verwerkte persoonsgegevens, hun lokalisaties en uitgevoerde verwerkingen;
- de nominatieve lijst van de organen of aangestelden die toegang hebben tot de gegevens;
- de configuratie van de systemen en netwerken;
- de technische documentatie over de ingestelde beheersmaatregelen;
- de agenda van geplande operaties;
- het opsporingsbeleid;
- de testplannen van de beheersmaatregelen;
- verslagen betreffende incidenten;
- eventuele auditverslagen.