

Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens¹

Het voorliggend document bevat een lijst met tien actiedomeinen in verband met de informatiebeveiliging waarvoor elke instelling – rechtspersoon², onderneming of administratie – die persoonsgegevens bewaart, 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 specifiek 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 wens 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. Veiligheidsbeleid

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

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

Het veiligheidsbeleid bestaat uit :

- een toelichting over de uitgevoerde analyse en het risicobeheer van de persoonsgegevens ;
- de prioriteiten die werden weerhouden en de mechanismen die ingevolge deze risicoanalyse werden of worden aangebracht ;
- de planning van de inwerkingstelling ;
- de beschrijving van de verschillende verantwoordelijkheden en de ingestelde organisatorische regels ,

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 persoonsgegevens van 8 december 1992.

² Dit stelt de natuurlijke personen niet vrij van de verplichting zich te voegen naar het artikel 16 van de wet tot bescherming van persoonsgegevens van 8 december 1992 die aan elke verantwoordelijke voor de verwerking verplichtingen oplegt inzake beveiliging.

³ Wet tot bescherming van de persoonsgegevens van 8 december 1992.

- de beschrijving van het beheersproces bij veiligheidsincidenten ,
- de beschrijving van het sensibiliseringsproces van de instelling voor dit beleid ;
- de weerhouden maatregelen om het veiligheidssysteem te actualiseren werken eens het werd geïnstalleerd.

Dit veiligheidsbeleid 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. Veiligheidsconsulent

Er moet binnen de instelling een veiligheidsconsulent worden aangesteld die verantwoordelijk is voor de uitvoering van het veiligheidsbeleid.

Rechtstreeks rapporterend aan de directie van de instelling, moet hij 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 veiligheidsbeleid blijft.

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

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

3. Organisatie en menselijke aspecten van de beveiliging

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

Om de beveiliging 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 classificatie⁴ van informatie. Dit maakt, ongeacht het soort drager, de inventarisatie en lokalisatie van alle verwerkte persoonsgegevens mogelijk.

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 beveiliging.

Er moeten eventueel 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 deze erop toezien dat in het contract van onderaanneming dezelfde verplichtingen inzake beveiliging opgenomen worden als deze die in de instelling zelf in voege zijn.

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.

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 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.

Wanneer een continuïteit van de diensten noodzakelijk blijkt, moeten er apparaten geïnstalleerd worden ter preventie, opsporing en aanpak van fysieke bedreigingen zoals branden of overstromingen. Deze 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 verwerking van persoonsgegevens, de vertrouwelijkheid en de integriteit van de gegevens garanderen.

Indien het intern 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 en kwaadaardige software etc).

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 verwerken en van hun respectievelijke machtigingen.

Deze verschillende machtigingen moeten vertaald worden in technische voorzieningen en toegangscontroles tot de verschillende informatica-elementen (programma's, procedures, de 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 de toegang

De instelling moet loggings- en opsporingsmechanismen installeren

Dit moet ingeval van noodzaak toelaten dat de identiteit kan worden teruggevonden van iedere persoon die toegang had tot de persoonsgegevens of van elke bewerking ervan. De registratie van deze controle-informatie kan naargelang het geval betrekking hebben op de fysieke toegang, de logische toegang of beide.

De fijnheid van de registraties, de lokalisatie, en de bewaarduur van deze, de frekwentie en het type bewerkingen, hangen af van de context. Bijkomende mechanismen voor opsporing van inbraak zouden kunnen vereist zijn. De veiligheidsconsulent moet in staat zijn de gedane keuzes te rechtvaardigen.

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

8. Toezicht, nazicht en onderhoud

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

Om de noden te kunnen opsporen die toelaten de veiligheid op een passend niveau te houden, 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 een 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 veiligheidsmaatregelen doorgevoerd worden.

9. Beheer van veiligheidsincidenten en continuïteit

De instelling moet beschikken over een beheersplan voor veiligheidsincidenten.

In geval 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 dergelijke situatie in de dijken. Hiertoe moet de instelling procedures voorzien die nauwkeurig omschrijven welke de te ondernemen stappen zijn bij de ontdekking van een veiligheidsincident van persoonsgegevens alsook wie de verantwoordelijke personen zijn die dit incident moeten aanpakken om dit in 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 incident te vermijden of om zo snel mogelijk naar de normale toestand te kunnen terugkeren.

De instellingen, verplicht om de continuïteit van hun diensten te verzekeren, moeten :

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

10. Documentatie

De instelling moet beschikken over een volledige, gecentraliseerde documentatie en deze met betrekking tot de veiligheid 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 veiligheidsbehoeften, voortdurend worden bijgewerkt, en geïnventariseerd op een wijze dat ze te zijner tijd beschikbaar is voor de bevoegde persoon.

Deze documentatie moet ten minste het volgende bevatten :

- Identiteit van de veiligheidsconsulent;
- Het veiligheidsbeleid;
- De implementatie van de beveiligingsmaatregelen
- De inventaris van de 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 veiligheidsmaatregelen;
- De agenda van de geplande operaties;
- Het opsporingsbeleid ;
- De testplannen van de beveiligingsmaatregelen
- De verslagen betreffende incidenten;
- De eventuele auditverslagen.