Actiepunten Privacy

1 Documenteren en in kaart brengen van alle verwerkingen van persoonsgegevens;
2 Hiaten in de gegevensbescherming en de rechtmatigheid van de verwerking in kaart brengen;
3 Privacybeleid opstellen in het kader van de informatieverplichting afhankelijk van de gegevensverwerking (zie #1);
4 Wijze van verkrijgen toestemming inventariseren en aanpassen waar nodig;
5 Inventariseren of betrokkenen hun rechten kunnen uitoefenen en waar nodig mogelijkheid om rechten uit te oefenen implementeren;
6 Mogelijkheid van dataportabiliteit onderzoeken;
7 Datalekprotocol opstellen, actieplan ontwikkelen, testen en implementeren;
8 Bewerkersovereenkomsten sluiten;
9 ICT-omgeving inventariseren en aanpassen waar nodig om te kunnen voldoen aan documentatieplicht, inzichtelijk maken van dataprocessen, adequate bescherming en adequate reactie op lek;
10 Taken binnen de organisatie en toegang tot persoonsgegevens afbakenen;
11 Aan de hand van #1 nagaan welke gegevensverwerking noodzakelijk is en welke verwerking een hoog risico met zich meebrengt. Indien nodig risicobeperkende maatregelen nemen;
12 Eventueel “cyberverzekering” afsluiten.

Op langere termijn moeten de volgende zaken regelmatig plaatsvinden:

- Audits om potentiële risicogebieden te onderkennen en oplossingen te implementeren;
- Intern beleid ontwikkelen en implementeren voor de bescherming van persoonsgegevens en deze regel matig controleren op naleving;
- Privacygevoelige processen definiëren en over de gehele laag van de organisatie risicobeperkende maatregelen nemen;
- Snelle reactie op bijv. datalekken mogelijk maken en proces regelmatig controleren (brandalarmoefening);
- Extra beveiliging voor bijzondere categorieën persoonsgegevens;
- Houd in de gaten of er gedragscodes of certificatiemechanismen in de branche worden goedgekeurd door de toezichthouder;
- Zorg voor bewustwording binnen de organisatie en diens medewerkers.