Onderstaand de fair Information principles uit de Algemene Verordening Gegevensbescherming (AVG)[1].

1. Rechtmatig
De gegevensverwerking moet rechtmatig zijn. Dat houdt twee dingen in. Ten eerste moet de gegevensverwerking stoelen op één van de gronden die in de Algemene Verordening Gegevensbescherming zijn genoemd. Ten tweede moet de gegevensverwerking uiteraard ook aan andere wetgeving voldoen, zoals de Grondwet, de Wet ongelijke behandeling en het Wetboek van Strafrecht.

2. Behoorlijk
De gegevensverwerking moet behoorlijk zijn. Behoorlijk is een wat gekunstelde vertaling van het Engels 'fair'. Hierbij kun je bijvoorbeeld denken aan oneerlijke handelspraktijken, waarbij de consument worden misleid, of aan 'unfair' terms and conditions, waarin de consument akkoord wordt gevraagd voor allerhande zaken die hij niet redelijkerwijs hoeft te verwachten.

3. Doelspecificatie
De gegevensverwerking moet een specifiek doel dienen.
a. Ten eerste betekent dit dat nog voordat er wordt aangevangen met het verwerken van persoonsgegevens er een doel moet worden afgesproken. Het is niet toegestaan persoonsgegevens te verzamelen en achteraf past vast te stellen waar die voor nodig zijn.
b. Ten tweede moet dat doel uitdrukkelijk zijn vastgelegd, zodat achteraf eenvoudig kan worden gecontroleerd of het oorspronkelijke doel inderdaad gerespecteerd is.
c. Tot slot moet het doel specifiek zijn. Veel organisaties gaan bij dit vereiste de mist in, omdat ze veel te brede en algemene doelen hebben geformuleerd, zoals 'klantencontact', 'productverbetering', 'innovatie' of 'reclamedoeleinden'. Deze doelen zijn te breed en zullen derhalve als onrechtmatig worden beoordeeld.

4. Doelbinding
Doelbinding: De gegevens mogen in principe alleen voor het vastgelegde doel worden verwerkt. Het gebruiken van al verzamelde gegevens voor nieuwe toepassingen is in principe niet toegestaan. Dit mag alleen als het doel gelijksoortig is.

5. Dataminimalisatie
Het uitgangspunt is dat er in principe zo min mogelijk persoonsgegevens worden verzameld. Het dataminimalisatie principe uit de AVG is in wezen een uitwerking van het algemene noodzakelijkheidsvereiste en subsidiariteitsprincipe. Het stelt simpelweg dat je niet meer persoonsgegevens mag verzamelen dan je strikt gezien nodig hebt voor het bereiken van je specifieke doel.

6. Correctheid
De gegevens die iemand verzamelt moeten correct zijn. Je moet bij het verzamelen van de persoonsgegevens dus goed nadenken over een onderzoeksmethodologie en waarborgen treffen voor een goede dataverzameling. Je kan niet zomaar lukraak gegevens over mensen verzamelen en daaruit wat willekeurige conclusies trekken. Dit principe is in de Algemene Verordening Gegevensbescherming vervat om ervoor zorg te dragen dat de analyse en uitkomsten van de gegevensverwerking correct zijn en dat de besluiten die daarop worden genomen adequaat en

[1] Afgeleid uit het boek van Bart van der Sloot:…..

eerlijk zijn. Een persoon mag bijvoorbeeld geen negatieve consequenties ondervinden van verkeerd geregistreerde gegevens.

7. Up to date
Als de persoonsgegevens voor een langere tijd worden bewaard, dan heb je de plicht om er voor te zorgen dat de gegevens up to date blijven. Voor gewone en alledaagse databases is een jaarlijkse update van de gegevens vaak voldoende, voor meer impactvolle beslissingen en gevoelige datasets moet dat vaker, bijvoorbeeld één keer per maand. Daarbij is het raadzaam om, voordat er specifieke beslissingen worden genomen op basis van de dataset ten aanzien van een specifiek persoon of kleine groep personen, individueel na te gaan of alle elementen in het stappenproces zorgvuldig zijn verlopen.

8. Verwijderen persoonsgegevens
Als je de persoonsgegevens die je hebt verzameld niet langer nodig hebt, bijvoorbeeld omdat je het doel waarvoor je ze hebt verzameld hebt bereikt, dan moet je ze in principe verwijderen of volledig anonimiseren. Het anonimiseren van een dataset heeft als voordeel ten opzichte van het verwijderen dat je nog algemene statische analyses kan uitvoeren.

9. Bewaar alleen voor archivering of onderzoek
Je mag persoonsgegevens alleen bewaren als ze niet meer noodzakelijk zijn voor het doel waarvoor je ze hebt verzameld als je ze nog nodig hebt voor het voldoen aan een wettelijke plicht, bijvoorbeeld de plicht om de belastingdienst inzage te geven in je administratie, of omdat je betrokken bent bij historisch of wetenschappelijk onderzoek, statistisch onderzoek of omdat je onder een archiveringsplicht valt. Onderzoek en statistische analyse heeft hier betrekking op wetenschappelijk en medisch onderzoek; de Algemene Verordening Gegevensbescherming noemt in dit verband het doen van klinische proeven, onderzoek op het gebied van de volksgezondheid en onderzoek waarbij er wordt gedaan aan maatschappelijke kennisvermeerdering.

10. Technologische veiligheid
Als de gegevens worden opgeslagen, bijvoorbeeld in een database, register of bestand, dan zul je technische veiligheidsmaatregelen moeten treffen.
Bijvoorbeeld:
- Versleuteling: Zorg dat hackers geen onbevoegde toegang kunnen krijgen tot de databases. Versleutel de persoonsgegevens dus goed en zorg dat er alarm wordt geslagen zodra er signalen zijn dat er pogingen zijn tot onbevoegde toegang.
- Automatische blokkade: Zorg dat als er drie keer een fout wachtwoord wordt ingevoerd, het apparaat dat poogt toegang te krijgen tot de database automatisch wordt geblokkeerd. Bij de verwerking van gevoelige persoonsgegevens gebeurt dit bij voorkeur al na één keer. Waarschuw direct de persoon wiens credentials mogelijk worden misbruikt.
- Voorlichting: Zorg dat je zowel je medewerkers als je relaties waarschuwt over de gevaren van hackers. Bekend is dat veel klanten en werknemers, ondanks de vele waarschuwingen, bijvoorbeeld toch trappen in mails die lijken te komen van een organisatie en waarin wordt gevraagd het wachtwoord te bevestigen of te wijzigen.
- Compartimenteren: Zorg dat je schotten plaatst tussen verschillende databases binnen je organisatie, die elk op een verschillende locatie staan, op verschillende servers staan en met verschillende technische maatregelen zijn beveiligd. Zo voorkom je dat als het hackers lukt een wachtwoord te bemachtigen en onbevoegd toegang te krijgen, zij slecht een klein deel van de gegevens kunnen zien en niet in een keer alle gegevens.
- Blokkades: Zorg dat als het toch fout gaat, er obstakels worden opgeworpen, zodat het bijvoorbeeld onmogelijk of lastig wordt gemaakt om de database in zijn geheel te kopiëren of te downloaden.
- Melding: Zorg dat als het toch fout gaat, je aan de meldplicht voldoet.

11. Organisatorische veiligheid
Als de gegevens worden opgeslagen, bijvoorbeeld in een database, register of bestand, dan zul je organisatorische veiligheidsmaatregelen moeten treffen om er voor te zorgen dat alleen personen binnen je organisatie toegang krijgen tot persoonsgegevens als zij die ook echt nodig hebben.
Bijvoorbeeld:
-Authenticatie: Zorg dat er alleen toegang kan worden verkregen tot persoonsgegevens, bestanden en databases door middel van een persoonlijke code.
-Beperking: Zorg dat alleen die personen binnen je organisatie authenticatie- en toegangsrechten krijgen die dat ook echt nodig hebben. Daarbij geldt als uitgangspunt dat hoe gevoeliger de persoonsgegeven en des te groter de dataset, des te minder mensen er toegang tot hebben.
-Logging: Hou goed bij wie er binnen je organisatie toegang heeft gekregen tot de persoonsgegevens. Bij voorkeur moeten de personen ook registreren waarom ze toegang hebben genomen tot de database, maar in ieder geval moeten zij dat kunnen verklaren.
-Automatisch uitloggen: Een andere maatregel kan zijn dat een computer waarop is ingelogd automatisch na een aantal minuten uitlogt als die niet meer wordt gebruikt.
-Clean desk: Ook doen steeds meer organisaties aan een clean-desk policy. Na sluitingstijd worden alle documenten die niet achter slot en grendel zijn opgeborgen in de versnipperaar gegooid of alsnog opgeborgen, om zo te voorkomen dat gevoelige informatie rondslingert.
-Fysieke beveiliging: kamers en bijzondere ruimtes op slot

12. Transparantie
Openheid over de gegevensverwerkingsprocessen binnen de organisatie is één van de pijlers van der Algemene Verordening Gegevensbescherming.
Voor alle informatie geldt dat die kosteloos moet worden verstrekt en in heldere en begrijpelijke taal moet worden gecommuniceerd. Er zijn drie vormen van transparantie die organisaties moeten betrachten en dat zijn:
Algemene openheid
Informatie aan de betrokkenen
Kennisgeving als er een beveiligingslek is